

Attachment(s): 3 Certified Copy(ies)

併合親 2002-332404  
US  
924

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 2 年 1 1 月 1 5 日

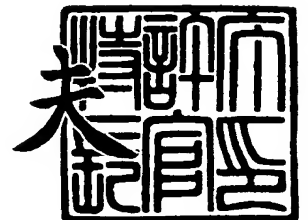
出 願 番 号  
Application Number: 特 願 2 0 0 2 - 3 3 2 4 0 5  
[ST. 10/C]: [ J P 2 0 0 2 - 3 3 2 4 0 5 ]

出 願 人  
Applicant(s): 日本電気株式会社  
日本電気通信システム株式会社

2 0 0 3 年 9 月 2 5 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 7 8 9 5 0

【書類名】 特許願

【整理番号】 49200233

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/08  
H04L 12/56  
G06F 13/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 鈴木 一哉

【発明者】

【住所又は居所】 東京都港区三田一丁目 4 番 2 8 号 日本電気通信システム株式会社内

【氏名】 馬越 英之

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 地引 昌弘

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【特許出願人】

【識別番号】 000232254

【氏名又は名称】 日本電気通信システム株式会社

【代理人】

【識別番号】 100088890

【弁理士】

【氏名又は名称】 河原 純一

【手数料の表示】

【予納台帳番号】 009690

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9001717

【包括委任状番号】 9002497

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 マルチキャスト配信のための鍵管理方式

【特許請求の範囲】

【請求項 1】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、  
コンテンツサーバ群とクライアント群とからアクセス可能となるように配置されており、暗号鍵・復号鍵と当該鍵を一意に識別するための鍵 ID との組を保持することによって鍵を管理する鍵管理サーバと、  
前記鍵管理サーバから暗号鍵とその鍵 ID との組を受け取り、当該暗号鍵で暗号化されたデータと当該鍵 ID とを有するマルチキャストパケットをクライアント群に送信するコンテンツサーバと、  
前記コンテンツサーバからマルチキャストパケットを受信し、当該マルチキャストパケットに含まれる鍵 ID に対応する復号鍵を前記鍵管理サーバから取得し、当該復号鍵によって当該マルチキャストパケットに含まれる暗号化データの復号化を行うクライアントと  
を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項 2】 鍵管理サーバを鍵管理マスターサーバと複数の鍵管理スレーブサーバとに分けることによって、負荷分散を可能にすることを特徴とする請求項 1 記載のマルチキャスト配信のための鍵管理方式。

【請求項 3】 コンテンツサーバが、使用する鍵を変更するときに、事前に鍵変更予告のマルチキャスト配信を行い、鍵管理サーバからの新たな復号鍵の取得をクライアントに促すことによって、鍵変更時にも遅延なく復号化を行うことを可能にすることを特徴とする請求項 1 または請求項 2 記載のマルチキャスト配信のための鍵管理方式。

【請求項 4】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、  
暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 ID との組を保持する鍵管理サーバ内の鍵管理テーブルと、  
コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該

鍵に鍵 I D を割り当て、生成した暗号鍵・復号鍵と当該鍵 I D との組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 I D との組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵管理サーバ内の鍵生成手段と、

クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する鍵管理サーバ内の復号鍵送付手段と、

暗号鍵とその鍵 I D との組を保持するコンテンツサーバ内の暗号鍵テーブルと、マルチキャスト配信時に、暗号鍵を取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 I D との組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、

前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、

復号鍵とその鍵 I D との組を保持するクライアント内の復号鍵テーブルと、マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵 I D に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には鍵管理サーバに対して当該鍵 I D をキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 I D との組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、

マルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段と

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項 5】 暗号化データのマルチキャスト配信が行われるネットワークシス

テムにおいて、

暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 I D との組を保持する鍵管理マスタサーバおよび鍵管理スレーブサーバ内の鍵管理テーブルと、

コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵 I D を割り当て、生成した暗号鍵・復号鍵と当該鍵 I D との組を鍵管理マスタサーバ内の前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 I D との組を有する鍵情報応答メッセージを当該コンテンツサーバに返送し、当該暗号鍵・復号鍵と当該鍵 I D との組を有する鍵情報配布メッセージを全ての鍵管理スレーブサーバに配布する鍵管理マスタサーバ内の鍵生成・配布手段と、

前記鍵生成・配布手段によって配布された鍵情報配布メッセージ中の暗号鍵・復号鍵と鍵 I D との組を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルに保存する鍵管理スレーブサーバ内の鍵保存手段と、

クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する鍵管理スレーブサーバ内の復号鍵送付手段と、

暗号鍵とその鍵 I D との組を保持するコンテンツサーバ内の暗号鍵テーブルと、マルチキャスト配信時に、暗号鍵を取得するために鍵管理マスタサーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 I D との組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、

前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、

復号鍵とその鍵 I D との組を保持するクライアント内の復号鍵テーブルと、マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵 I D に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には全ての鍵管理スレーブサ

ーバのいずれかに対して当該鍵 I D をキーにした鍵情報要求を送信し、その鍵情報要求の返信として当該鍵管理スレーブサーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 I D との組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、

マルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段と

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項 6】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 I D との組を保持する鍵管理サーバ内の鍵管理テーブルと、

コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵 I D を割り当て、生成した暗号鍵・復号鍵と当該鍵 I D との組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 I D との組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵管理サーバ内の鍵生成手段と、

クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する鍵管理サーバ内の復号鍵送付手段と、

暗号鍵とその鍵 I D との組を保持するコンテンツサーバ内の暗号鍵テーブルと、  
鍵変更準備時点に達した時に、次に使用する暗号鍵を事前に取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 I D との組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、

前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、



前記暗号鍵取得手段によって次に使用する暗号鍵の取得が行われた場合に、当該暗号鍵の鍵 I D を有する鍵変更予告メッセージのマルチキャスト配信を行うコンテンツサーバ内の鍵変更予告手段と、

復号鍵とその鍵 I D との組を保持するクライアント内の復号鍵テーブルと、  
鍵変更予告メッセージの受信時に、当該鍵変更予告メッセージ中の鍵 I D に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がない場合に鍵管理サーバに対して当該鍵 I D をキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 I D との組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、

マルチキャストパケットを受信し、前記復号鍵取得手段により事前に取得され前記復号鍵管理テーブルに保持されており当該マルチキャストパケット中の鍵 I D に対応する復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段と

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項 7】 コンテンツサーバ側で、複数の暗号鍵と鍵 I D との組を同時に保持しており、マルチキャスト配信において使用する暗号鍵を適時変更することを可能ならしめることを特徴とする請求項 1，請求項 2，請求項 3，請求項 4，請求項 5，または請求項 6 記載のマルチキャスト配信のための鍵管理方式。

【請求項 8】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

鍵管理サーバを、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 I D との組を保持する鍵管理テーブル、コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵 I D を割り当て、生成した暗号鍵・復号鍵と当該鍵 I D との組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 I D との組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵生成手段、およびクライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する復号鍵送付手段とし

て機能させるための鍵管理サーバ用鍵管理プログラムと、  
コンテンツサーバを、暗号鍵とその鍵 ID との組を保持する暗号鍵テーブル、マルチキャスト配信時に、暗号鍵を取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 ID との組を前記暗号鍵テーブルに保存する暗号鍵取得手段、および前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 ID とを有するマルチキャストパケットの送信を行う暗号化・送信手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、  
クライアントを、復号鍵とその鍵 ID との組を保持する復号鍵テーブル、マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵 ID に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には鍵管理サーバに対して当該鍵 ID をキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 ID との組を前記復号鍵テーブルに保存する復号鍵取得手段、およびマルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行う受信・復号化手段として機能させるためのクライアント用鍵管理プログラムと  
を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項 9】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

鍵管理マスタサーバを、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 ID との組を保持する鍵管理テーブル、およびコンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵 ID を割り当て、生成した暗号鍵・復号鍵と当該鍵 ID との組を鍵管理マスタサーバ内の前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 ID との組を有する鍵情報応答メッセージを当該コンテンツサーバに返送し、当該暗号鍵・復号鍵と当該鍵 ID との組を有する鍵情報配布メッセージを全ての鍵管理スレーブサーバに配布する鍵生成・配布手段と

して機能させるための鍵管理マスタサーバ用鍵管理プログラムと、  
鍵管理スレーブサーバを、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 I D との組を保持する鍵管理テーブル、前記鍵生成・配布手段によって配布された鍵情報配布メッセージ中の暗号鍵・復号鍵と鍵 I D との組を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルに保存する鍵保存手段、およびクライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する復号鍵送付手段として機能させるための鍵管理スレーブサーバ用鍵管理プログラムと、

コンテンツサーバを、暗号鍵とその鍵 I D との組を保持する暗号鍵テーブル、マルチキャスト配信時に、暗号鍵を取得するために鍵管理マスタサーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 I D との組を前記暗号鍵テーブルに保存する暗号鍵取得手段、および前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットの送信を行う暗号化・送信手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、

クライアントを、復号鍵とその鍵 I D との組を保持する復号鍵テーブル、マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵 I D に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には全ての鍵管理スレーブサーバのいずれかに対して当該鍵 I D をキーにした鍵情報要求を送信し、その鍵情報要求の返信として当該鍵管理スレーブサーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 I D との組を前記復号鍵テーブルに保存する復号鍵取得手段、およびマルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行う受信・復号化手段として機能させるためのクライアント用鍵管理プログラムと

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項 1 0】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

鍵管理サーバを、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 I D との組を保持する鍵管理テーブル、コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵 I D を割り当て、生成した暗号鍵・復号鍵と当該鍵 I D との組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 I D との組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵生成手段、およびクライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する復号鍵送付手段として機能させるための鍵管理サーバ用鍵管理プログラムと、

コンテンツサーバを、暗号鍵とその鍵 I D との組を保持する暗号鍵テーブル、鍵変更準備時点に達した時に、次に使用する暗号鍵を事前に取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 I D との組を前記暗号鍵テーブルに保存する暗号鍵取得手段、前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットの送信を行う暗号化・送信手段、および前記暗号鍵取得手段によって次に使用する暗号鍵の取得が行われた場合に、当該暗号鍵の鍵 I D を有する鍵変更予告メッセージのマルチキャスト配信を行う鍵変更予告手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、

クライアントを、復号鍵とその鍵 I D との組を保持する復号鍵テーブル、鍵変更予告メッセージの受信時に、当該鍵変更予告メッセージ中の鍵 I D に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がない場合に鍵管理サーバに対して当該鍵 I D をキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 I D との組を前記復号鍵テーブルに保存する復号鍵取得手段、お

よびマルチキャストパケットを受信し、前記復号鍵取得手段により事前に取得され前記復号鍵管理テーブルに保持されており当該マルチキャストパケット中の鍵 I D に対応する復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行う受信・復号化手段として機能させるためのクライアント用鍵管理プログラムと

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

**【発明の詳細な説明】**

**【0 0 0 1】**

**【発明の属する技術分野】**

本発明は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて暗号化／復号化で用いられる鍵（暗号鍵／復号鍵）の管理を行うマルチキャスト配信のための鍵管理方式に関する。

**【0 0 0 2】**

**【従来の技術】**

ユニキャスト通信における暗号化データの通信のためのプロトコルとして、I P s e c 等があるが、これらはそのままではマルチキャスト通信（配信）には適用できない。ユニキャスト通信は一対一で行われるため、二者間で鍵を共有すればよいが、マルチキャスト通信では一対多の通信になるため、ユニキャスト通信と同じ方法では鍵の共有ができないからである。このため、マルチキャスト通信における暗号化では、ユニキャスト通信におけるそれとは別のしくみが必要になる。

**【0 0 0 3】**

一般に、複数のマルチキャスト配信が行われている場合に、それぞれを区別するためには、送信元アドレス、マルチキャストアドレス、および送受信ポート番号の組合せによって、その区別が行われている。

**【0 0 0 4】**

したがって、従来の技術では、コンテンツサーバが複数あり、それぞれが違う鍵を用いて暗号化されたデータを含むマルチキャストパケットを配信している場合において、クライアント側では、それぞれのマルチキャストパケットに対応した

復号鍵を得るために、送信元アドレス、マルチキャストアドレス、および送受信ポート番号の組合せでマルチキャストパケットを区別する必要があった。

#### 【0 0 0 5】

また、暗号化データ（暗号化されたデータ）のマルチキャスト配信中に鍵（暗号鍵・復号鍵）を変える場合には、なんらかの方法を用いて、コンテンツサーバとクライアントとの間で、使用している暗号鍵・復号鍵の同期をとる必要がある。

#### 【0 0 0 6】

ここで、従来の技術では、鍵の同期を行う方式として、次のような処理を行う鍵管理サーバを利用して当該同期を実現するシステムが存在した（例えば、特許文献 1 参照）。

#### 【0 0 0 7】

すなわち、特許文献 1 に記載された鍵管理サーバは、送信者（コンテンツサーバ）が送信を始める際か鍵を変更した際に新しい鍵を受け取り、それを受信者（クライアント）に対して通知することで、送信データ（配信対象のデータ）に対応する鍵を受信者に配布している。

#### 【0 0 0 8】

##### 【特許文献 1】

特開 2 0 0 2 - 1 1 1 6 4 9 号公報（第 4 - 5 頁、図 1）

#### 【0 0 0 9】

##### 【発明が解決しようとする課題】

上述した従来のマルチキャスト配信のための鍵管理方式には、鍵が変更された際に、鍵管理サーバがクライアントに対して新しい鍵を配布する必要があり、このような鍵の管理を実現するために、現時点でマルチキャストパケット受信中のクライアントを鍵管理サーバが把握しておく必要がある等、鍵の管理が煩雑になるという問題点があった。

#### 【0 0 1 0】

本発明の目的は、上述の点に鑑み、マルチキャスト配信時に暗号化処理を行うネットワークシステムにおいて、事前に複数の鍵（暗号鍵・復号鍵）を一意に区別するための鍵 ID（送信者（コンテンツサーバ）と多数の受信者（クライアント

）との間で共有する鍵を区別する ID ( I D e n t i f i c a t i o n ) ) を鍵毎に割り当てておき、マルチキャスト配信の際に、配信対象のデータの暗号化に用いた鍵に対応する鍵 ID をマルチキャストパケットに包含して送り、そのような鍵 ID を使用して鍵の管理を実現することによって、鍵の管理を容易に行うことを可能にするマルチキャスト配信のための鍵管理方式を提供することにある。

#### 【0011】

すなわち、本発明を用いれば、コンテンツサーバが暗号鍵を変えた時に、コンテンツサーバが暗号化データに添付する鍵 ID を変えるだけで、クライアントは受信したマルチキャストパケット中の鍵 ID をみることによって、暗号化・復号化に用いる鍵が変わったことを知ることができ、クライアント側から鍵管理サーバ側に新しい鍵を要求できるため、鍵管理サーバ側でクライアントに関する情報を管理する必要がなくなる。

#### 【0012】

なお、IPsec 等のプロトコル（ユニキャスト通信のためのプロトコル）でも複数の鍵を区別するために ID が用いられるが、それはあくまでも二者間で共有されている鍵を区別するためのものである。

#### 【0013】

また、PKI ( P u b l i c   K e y   I n f r a s t r u c t u r e ) を用いた IPsec 通信では公開鍵を CA ( C e r t i f i c a t i o n   A u t h o r i t y ) 局と呼ばれるサーバにて保存しておき、クライアントが通信に先だってサーバから公開鍵を取得するということが行われるが、この公開鍵は通信のための共有鍵を交換するために用いられており、その公開鍵を使って暗号化通信を行うわけではない（本発明では、復号鍵およびその鍵 ID が鍵管理サーバからクライアントに渡される）。

#### 【0014】

##### 【課題を解決するための手段】

本発明のマルチキャスト配信のための鍵管理方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵（対となる暗号鍵および復号鍵。同じ鍵である場合もある）と当該鍵を一意に区別するため

の鍵 I D との組を保持する鍵管理サーバ内の鍵管理テーブルと、コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵 I D を割り当て、生成した暗号鍵・復号鍵と当該鍵 I D との組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 I D との組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵管理サーバ内の鍵生成手段と、クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する鍵管理サーバ内の復号鍵送付手段と、暗号鍵とその鍵 I D との組を保持するコンテンツサーバ内の暗号鍵テーブルと、マルチキャスト配信時に、暗号鍵を取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 I D との組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、復号鍵とその鍵 I D との組を保持するクライアント内の復号鍵テーブルと、マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵 I D に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には鍵管理サーバに対して当該鍵 I D をキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 I D との組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、マルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段とを有する。

#### 【0015】

ここで、本発明のマルチキャスト配信のための鍵管理方式は、上記の鍵管理サーバを、上記の鍵管理テーブル、鍵生成手段、および復号鍵送付手段として機能させるための鍵管理サーバ用鍵管理プログラムと、上記のコンテンツサーバを、上



記の暗号鍵テーブル、暗号鍵取得手段、および暗号化・送信手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、上記のクライアントを、上記の復号鍵テーブル、復号鍵取得手段、および受信・復号化手段として機能させるためのクライアント用鍵管理プログラムとを有する態様で実現することも可能である。

#### 【0 0 1 6】

また、本発明のマルチキャスト配信のための鍵管理方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 I D との組を保持する鍵管理マスタサーバおよび鍵管理スレーブサーバ内の鍵管理テーブルと、コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵 I D を割り当て、生成した暗号鍵・復号鍵と当該鍵 I D との組を鍵管理マスタサーバ内の前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 I D との組を有する鍵情報応答メッセージを当該コンテンツサーバに返送し、当該暗号鍵・復号鍵と当該鍵 I D との組を有する鍵情報配布メッセージを全ての鍵管理スレーブサーバに配布する鍵管理マスタサーバ内の鍵生成・配布手段と、前記鍵生成・配布手段によって配布された鍵情報配布メッセージ中の暗号鍵・復号鍵と鍵 I D との組を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルに保存する鍵管理スレーブサーバ内の鍵保存手段と、クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する鍵管理スレーブサーバ内の復号鍵送付手段と、暗号鍵とその鍵 I D との組を保持するコンテンツサーバ内の暗号鍵テーブルと、マルチキャスト配信時に、暗号鍵を取得するために鍵管理マスタサーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 I D との組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットの送信を行うコンテンツサーバ

内の暗号化・送信手段と、復号鍵とその鍵 I D との組を保持するクライアント内の復号鍵テーブルと、マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵 I D に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には全ての鍵管理スレーブサーバのいずれかに対して当該鍵 I D をキーにした鍵情報要求を送信し、その鍵情報要求の返信として当該鍵管理スレーブサーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 I D との組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、マルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段とを有するように構成することも可能である。

#### 【0 0 1 7】

ここで、本発明のマルチキャスト配信のための鍵管理方式は、上記の鍵管理マスターサーバを、上記の鍵管理テーブルおよび鍵生成・配布手段として機能させるための鍵管理マスターサーバ用鍵管理プログラムと、上記の鍵管理スレーブサーバを、上記の鍵管理テーブル、鍵保存手段、および復号鍵送付手段として機能させるための鍵管理スレーブサーバ用鍵管理プログラムと、上記のコンテンツサーバを、上記の暗号鍵テーブル、暗号鍵取得手段、および暗号化・送信手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、上記のクライアントを、上記の復号鍵テーブル、復号鍵取得手段、および受信・復号化手段として機能させるためのクライアント用鍵管理プログラムとを有する態様で実現することも可能である。

#### 【0 0 1 8】

さらに、本発明のマルチキャスト配信のための鍵管理方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵 I D との組を保持する鍵管理サーバ内の鍵管理テーブルと、コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵 I D を割り当て、生成した暗号鍵・復号鍵と当該鍵 I D との組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵 I D との組を有する鍵情

報応答メッセージを当該コンテンツサーバに返送する鍵管理サーバ内の鍵生成手段と、クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵 I D に対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵 I D との組を有する鍵情報メッセージを当該クライアントに返送する鍵管理サーバ内の復号鍵送付手段と、暗号鍵とその鍵 I D との組を保持するコンテンツサーバ内の暗号鍵テーブルと、鍵変更準備時点に達した時に、次に使用する暗号鍵を事前に取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵 I D との組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、前記暗号鍵取得手段によって次に使用する暗号鍵の取得が行われた場合に、当該暗号鍵の鍵 I D を有する鍵変更予告メッセージのマルチキャスト配信を行うコンテンツサーバ内の鍵変更予告手段と、復号鍵とその鍵 I D との組を保持するクライアント内の復号鍵テーブルと、鍵変更予告メッセージの受信時に、当該鍵変更予告メッセージ中の鍵 I D に対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がない場合に鍵管理サーバに対して当該鍵 I D をキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵 I D との組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、マルチキャストパケットを受信し、前記復号鍵取得手段により事前に取得され前記復号鍵管理テーブルに保持されており当該マルチキャストパケット中の鍵 I D に対応する復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段とを有するように構成することも可能である。

#### 【 0 0 1 9 】

ここで、本発明のマルチキャスト配信のための鍵管理方式は、上記の鍵管理サーバを、上記の鍵管理テーブル、鍵生成手段、および復号鍵送付手段として機能させるための鍵管理サーバ用鍵管理プログラムと、上記のコンテンツサーバを、上

記の暗号鍵テーブル、暗号鍵取得手段、暗号化・送信手段、および鍵変更予告手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、上記のクライアントを、上記の復号鍵テーブル、復号鍵取得手段、および受信・復号化手段として機能させるためのクライアント用鍵管理プログラムとを有する態様で実現することも可能である。

#### 【0020】

なお、本発明のマルチキャスト配信のための鍵管理方式は、より一般的には、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、コンテンツサーバ群とクライアント群とからアクセス可能となるように配置されており、暗号鍵・復号鍵と当該鍵を一意に識別するための鍵IDとの組を保持することによって鍵を管理する鍵管理サーバと、前記鍵管理サーバから暗号鍵とその鍵IDとの組を受け取り、当該暗号鍵で暗号化されたデータと当該鍵IDとを有するマルチキャストパケットをクライアント群に送信するコンテンツサーバと、前記コンテンツサーバからマルチキャストパケットを受信し、当該マルチキャストパケットに含まれる鍵IDに対応する復号鍵を前記鍵管理サーバから取得し、当該復号鍵によって当該マルチキャストパケットに含まれる暗号化データの復号化を行うクライアントとを有すると表現することができる。

#### 【0021】

ここで、このマルチキャスト配信のための鍵管理方式に関しては、鍵管理サーバを鍵管理マスターサーバと複数の鍵管理スレーブサーバとに分けることによって、負荷分散を可能にすることもできる。また、コンテンツサーバが、使用する鍵を変更するときに、事前に鍵変更予告のマルチキャスト配信を行い、鍵管理サーバからの新たな復号鍵の取得をクライアントに促すことによって、鍵変更時にも遅延なく復号化を行うことを可能にすることもできる。

#### 【0022】

##### 【発明の実施の形態】

次に、本発明について図面を参照して詳細に説明する。

#### 【0023】

##### (1) 第1の実施の形態

**【0024】**

図1は、本発明の第1の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

**【0025】**

図1を参照すると、本実施の形態に係るマルチキャスト配信のための鍵管理方式は、マルチキャストパケットを送信するコンテンツサーバ11, 12, ..., 1n (nは正整数)と、マルチキャストパケットを受信するクライアント21, 22, ..., 2m (mは正整数)と、鍵(暗号鍵・復号鍵)の管理を行う鍵管理サーバ31と、コンテンツサーバ1i (iは1~nの正整数), クライアント2j (jは1~mの正整数), および鍵管理サーバ31を接続するネットワーク100とを含んで構成されている。

**【0026】**

コンテンツサーバ1iは、マルチキャストパケットで配信されるデータの暗号化に用いる鍵(暗号鍵)とその鍵を識別するための鍵IDとの組を保存する暗号鍵テーブル1i0を持つ。

**【0027】**

また、各コンテンツサーバ1iは、暗号鍵取得手段1i1と、暗号化・送信手段1i2とを含んで構成されている。

**【0028】**

クライアント2jは、マルチキャストパケットで配信される暗号化データの復号に用いる鍵(復号鍵)とその鍵を識別するための鍵IDとの組を保存する復号鍵テーブル2j0を持つ。

**【0029】**

また、各クライアント2jは、復号鍵取得手段2j1と、受信・復号化手段2j2とを含んで構成されている。

**【0030】**

鍵管理サーバ31は、鍵(暗号鍵・復号鍵)とそれに対応する鍵IDとの組を管理する鍵管理テーブル310を持つ。なお、一対の暗号化・復号化処理で用いられる暗号鍵と復号鍵とは、暗号化方式によって、同一の場合もあり異なる場合も

あるが、いずれにしても同一の鍵IDによって識別される。

#### 【0031】

また、鍵管理サーバ31は、鍵生成手段311と、復号鍵送付手段312とを含んで構成されている。

#### 【0032】

図2は、本実施の形態に係るマルチキャスト配信のための鍵管理方式の動作を説明するためのブロック図である。図2に示すように、コンテンツサーバ1iから鍵管理サーバ31に鍵作成要求51が送信され、その応答として、鍵管理サーバ31からコンテンツサーバ1iに鍵情報応答メッセージ52が送信される。また、クライアント2jから鍵管理サーバ31に鍵情報要求61が送信され、その応答として、鍵管理サーバ31からクライアント2jに鍵情報メッセージ62が送信される。

#### 【0033】

図3は、本実施の形態に係るマルチキャスト配信のための鍵管理方式における暗号化・送信処理を示す流れ図である。この処理は、暗号鍵有無判定ステップA1と、鍵作成要求発行ステップA2と、鍵生成ステップA3と、鍵ID割り当てステップA4と、鍵情報鍵管理テーブル保存ステップA5と、鍵情報応答メッセージ送信ステップA6と、鍵情報暗号鍵テーブル保存ステップA7と、データ暗号化ステップA8と、鍵ID保有マルチキャストパケット生成ステップA9と、マルチキャストパケット送信ステップA10とからなる。

#### 【0034】

図4は、本実施の形態に係るマルチキャスト配信のための鍵管理方式における受信・復号化処理を示す流れ図である。この処理は、マルチキャストパケット受信ステップB1と、復号鍵有無判定ステップB2と、鍵情報要求発行ステップB3と、鍵管理テーブル検索ステップB4と、鍵情報メッセージ送信ステップB5と、鍵情報復号鍵テーブル保存ステップB6と、暗号化データ復号化ステップB7とからなる。

#### 【0035】

次に、図1～図4を参照して、上記のように構成された本実施の形態に係るマル

マルチキャスト配信のための鍵管理方式の全体の動作について詳細に説明する。

#### 【0036】

第1に、コンテンツサーバ側における暗号化・送信処理時の動作について説明する（図3参照）。

#### 【0037】

コンテンツサーバ1 i 内の暗号化・送信手段1 i 2 は、配信対象のデータを暗号化してその暗号化データを有するマルチキャストパケットを送信する際に、その暗号化のための鍵（暗号鍵）が当該コンテンツサーバ1 i の暗号鍵テーブル2 i 0（自テーブル）に保持されているか否かを判定する（ステップA1）。

#### 【0038】

暗号化・送信手段1 i 2 は、ステップA1で「当該暗号鍵が自テーブルに保持されている」と判定した場合には、その暗号鍵を用いて配信対象のデータの暗号化を行い（ステップA8）、その暗号化データと当該暗号鍵に対応する鍵IDとを有するマルチキャストパケットを生成し（ステップA9）、ネットワーク100上への当該マルチキャストパケットの送信（マルチキャスト配信）を行う（ステップA10）。

#### 【0039】

一方、暗号化・送信手段1 i 2 は、ステップA1で「当該暗号鍵が自テーブルに保持されていない」と判定した場合には、暗号鍵取得手段1 i 1 に制御を渡す。暗号鍵取得手段1 i 1 は、鍵管理サーバ31に対して鍵作成要求51（図2参照）を発行する（ステップA2）。

#### 【0040】

鍵作成要求51を受け取った鍵管理サーバ31内の鍵生成手段311は、要求された鍵（暗号鍵・復号鍵）を生成し（ステップA3）、その鍵に対して、鍵管理テーブル310内で一意に管理するための鍵IDを割り当てる（ステップA4）。

#### 【0041】

さらに、鍵生成手段311は、ステップA3で生成した鍵とステップA4で割り当てた鍵IDとの組を鍵管理テーブル310に保存し（ステップA5）、鍵作成

要求 5 1 の発行元のコンテンツサーバ 1 i に対して当該鍵 I D と当該鍵（暗号鍵）との組を有する鍵情報応答メッセージ 5 2（図 2 参照）を送信する（ステップ A 6）。

【0 0 4 2】

鍵情報応答メッセージ 5 2 を受信したコンテンツサーバ 1 i 内の暗号鍵取得手段 1 i 1 は、受け取った鍵と鍵 I D との組を自身の暗号鍵テーブル 1 i 0 に保存する（ステップ A 7）。

【0 0 4 3】

さらに、当該コンテンツサーバ 1 i 内の暗号化・送信手段 1 i 2 は、鍵管理サーバ 3 1 から受け取った暗号鍵を用いて配信対象のデータの暗号化を行い（ステップ A 8）、その暗号化データと当該暗号鍵に対応する鍵 I D とを有するマルチキャストパケットを生成し（ステップ A 9）、ネットワーク 1 0 0 上への当該マルチキャストパケットの送信（マルチキャスト配信）を行う（ステップ A 1 0）。

【0 0 4 4】

なお、図 2 に示すコンテンツサーバ 1 2 のように、暗号鍵テーブル（図 2 では暗号鍵テーブル 1 2 0）内に複数の鍵が保持されている場合には、マルチキャスト配信の対象となるデータの内容や時刻によって当該複数の鍵を使い分けることも可能である。すなわち、本実施の形態に限らず、本発明では、コンテンツサーバ側で、複数の暗号鍵と鍵 I D との組を同時に保持しておき、マルチキャスト配信において使用する暗号鍵を適時変更することも可能である。

【0 0 4 5】

第 2 に、クライアント側における受信・復号化処理時の動作について説明する（図 4 参照）。

【0 0 4 6】

クライアント 2 j 内の受信・復号化手段 2 j 2 は、コンテンツサーバ 1 i から配信されたマルチキャストパケットを受信すると（ステップ B 1）、当該マルチキャストパケットに含まれる鍵 I D を参照し、当該鍵 I D に対応する鍵（復号鍵）が自身の復号鍵テーブル 8 j（自テーブル）にあるか否かを判定（検索）する（ステップ B 2）。



**【0047】**

受信・復号化手段 2 j 2 は、ステップ B 2 の検索で「当該鍵 ID に対応する復号鍵がある」と判定した場合には、その復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行う（ステップ B 7）。

**【0048】**

一方、受信・復号化手段 2 j 2 は、ステップ B 2 の検索で「当該鍵 ID に対応する復号鍵がない」と判定した場合には、復号鍵取得手段 2 j 1 に制御を渡す。復号鍵取得手段 2 j 1 は、当該マルチキャストパケットに含まれる鍵 ID を使って（当該鍵 ID をキーにして）、鍵情報要求 6 1（図 2 参照）を鍵管理サーバ 3 1 に発行する（ステップ B 3）。すなわち、当該鍵 ID に対応する復号鍵に関する鍵情報（鍵 ID と復号鍵との組）を、鍵管理サーバ 3 1 に対して要求する。

**【0049】**

その鍵情報要求 6 1 を受け取った鍵管理サーバ 3 1 内の復号鍵送付手段 3 1 2 は、鍵情報要求 6 1 中の鍵 ID を用いて鍵管理テーブル 3 1 0 の検索を行い、当該鍵 ID に対応する鍵を取得する（ステップ B 4）。

**【0050】**

その上で、復号鍵送付手段 3 1 2 は、鍵管理テーブル 3 1 0 から取得した鍵（復号鍵）とその鍵 ID との組を有する鍵情報メッセージ 6 2（図 2 参照）を、鍵情報要求 6 1 に対する返信として、鍵情報要求 6 1 を発行したクライアント 2 j に送信する（ステップ B 5）。

**【0051】**

当該クライアント 2 j 内の復号鍵取得手段 2 j 1 は、当該鍵情報メッセージ 6 2 を鍵管理サーバ 3 1 から受け取ると、以降のマルチキャストパケット受信時の復号化処理の際に用いるために、当該鍵情報メッセージ 6 2 中の復号鍵と鍵 ID との組を自身の復号鍵テーブル 2 j 0 に保存しておく（ステップ B 6）。

**【0052】**

さらに、当該クライアント 2 j 内の受信・復号化手段 2 j 2 は、その復号鍵を用いて、ステップ B 1 で受信したマルチキャストパケット中の暗号化データの復号化を行う（ステップ B 7）。

**【0 0 5 3】**

なお、クライアント 2 j の復号鍵テーブル 2 j 0 は、初期状態では 1 つの鍵情報（鍵 I D と鍵との組）も持っていない。また、復号鍵テーブル 2 j 0 中の鍵とその鍵 I D との組は、一定時間用いられないと、復号鍵テーブル 2 j 0 から消去される。

**【0 0 5 4】**

(2) 第 2 の実施の形態

**【0 0 5 5】**

図 5 は、本発明の第 2 の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

**【0 0 5 6】**

図 5 を参照すると、本実施の形態に係るマルチキャスト配信のための鍵管理方式は、マルチキャストパケットを送信するコンテンツサーバ 1 1, 1 2, …, 1 n (n は正整数) と、マルチキャストパケットを受信するクライアント 2 1, 2 2, …, 2 m (m は正整数) と、鍵（暗号鍵・復号鍵）の管理を行う鍵管理マスタ (MASTER) サーバ 4 0 および鍵管理スレーブ (SLAVE) サーバ 4 1, …, 4 p (p は正整数) と、コンテンツサーバ 1 i (i は 1 ~ n の正整数), クライアント 2 j (j は 1 ~ m の正整数), 鍵管理マスタサーバ 4 0, および鍵管理スレーブサーバ 4 k (k は 1 ~ p の正整数) を接続するネットワーク 1 0 0 とを含んで構成されている。

**【0 0 5 7】**

本実施の形態（第 2 の実施の形態）と第 1 の実施の形態とを比較すると、第 1 の実施の形態（図 1 参照）における鍵管理サーバ 3 1 に対応するものとして、本実施の形態では、鍵管理マスタサーバ 4 0 と複数の鍵管理スレーブサーバ 4 k とが分かれて存在している点が異なっている。

**【0 0 5 8】**

すなわち、図 5 に示す本実施の形態の構成は、鍵管理サーバを鍵管理マスタサーバ 4 0 と鍵管理スレーブサーバ 4 k とに分けて、鍵管理スレーブサーバ 4 k を複数用意することによって、鍵管理サーバの負荷の分散を可能にしている。

**【0 0 5 9】**

なお、鍵管理マスターサーバ4 0 は、鍵管理テーブル4 0 0 を有しており、鍵生成・配布手段4 0 1 を含んで構成されている。

**【0 0 6 0】**

また、鍵管理スレーブサーバ4 k は、鍵管理テーブル4 k 0 を有しており、鍵保存手段4 k 1 と、復号鍵送付手段4 k 2 とを含んで構成されている。

**【0 0 6 1】**

図6 は、本実施の形態に係るマルチキャスト配信のための鍵管理方式の動作を説明するためのブロック図である。図6 に示すように、コンテンツサーバ1 i（図6 では、簡単化のためにコンテンツサーバ1 1 のみを示している）から鍵管理マスターサーバ4 0 に鍵作成要求5 1 が送信され、その応答として、鍵管理マスターサーバ4 0 からコンテンツサーバ1 i に鍵情報応答メッセージ5 2 が送信される。このときに、鍵管理マスターサーバ4 0 から鍵管理スレーブサーバ4 1 ～4 p に鍵情報配布メッセージ7 1 ～7 p が送信される。また、クライアント2 j から鍵管理スレーブサーバ4 1 ～4 p のいずれかに鍵情報要求6 1 が送信され、その応答として、当該鍵管理スレーブサーバ4 k からクライアント2 j に鍵情報メッセージ6 2 が送信される。

**【0 0 6 2】**

次に、図5 および図6 を参照して（図1 ～図4 も適宜参照する）、上記のように構成された本実施の形態に係るマルチキャスト配信のための鍵管理方式の動作について、第1 の実施の形態とは異なる点を中心にして説明する。

**【0 0 6 3】**

第1 に、暗号化・送信処理時の動作について説明する。

**【0 0 6 4】**

第1 の実施の形態では、コンテンツサーバ1 i は、図3 中のステップA 1 で「暗号鍵が自テーブルに保持されていない」と判定した場合に、ステップA 2 で、鍵管理サーバ3 1 に鍵作成要求5 1（図2 参照）を発行していた。

**【0 0 6 5】**

これに対して、本実施の形態では、コンテンツサーバ1 i（コンテンツサーバi

1 内の暗号鍵取得手段 1 i 1) は、鍵管理マスタサーバ 4 0 に対して、鍵作成要求 5 1 (図 6 参照) を発行する。

#### 【0066】

そして、鍵作成要求 5 1 を受け取った鍵管理マスタサーバ 4 0 内の鍵生成・配布手段 4 0 1 は、鍵 (暗号鍵・復号鍵) を生成し、その鍵に対して、鍵管理テーブル 4 0 0 内で一意に管理するための鍵 ID を割り当てる。

#### 【0067】

また、鍵生成・配布手段 4 0 1 は、生成した鍵とその鍵に割り当てた鍵 ID との組を鍵管理テーブル 4 0 0 に保存し、鍵作成要求 5 1 に対する応答として、当該コンテンツサーバ 1 i に対して当該鍵 ID と当該鍵 (暗号鍵) との組を有する鍵情報応答メッセージ 5 2 (図 6 参照) を送信する。

#### 【0068】

さらに、鍵管理マスタサーバ 4 0 内の鍵生成・配布手段 4 0 1 は、この鍵と鍵 ID との組を有する鍵情報配布メッセージ 7 1 ~ 7 p (図 6 参照) を、全ての鍵管理スレーブサーバ 4 1 ~ 4 p に対しても送る。

#### 【0069】

各鍵管理スレーブサーバ 4 k 内の鍵保存手段 4 k 1 は、当該鍵と当該鍵 ID との組を、自己の鍵管理テーブル 4 k 0 に保存する。

#### 【0070】

第 2 に、受信・復号化処理時の動作について説明する。

#### 【0071】

第 1 の実施の形態では、クライアント 2 j は、図 4 中のステップ B 2 の検索 (判定) で「マルチキャストパケット中の鍵 ID に対応する復号鍵が自テーブルにない」と判定した場合には、ステップ B 3 で、コンテンツサーバ 1 i から受け取ったマルチキャストパケットに含まれている鍵 ID を使って、鍵情報要求 6 1 (図 2 参照) を鍵管理サーバ 3 1 に発行していた。

#### 【0072】

これに対して、本実施の形態では、クライアント 2 j は、鍵情報要求 6 1 (図 6 参照) を発行する時に、複数の鍵管理スレーブサーバ 4 1 ~ 4 p のいずれかにそ

の鍵情報要求 6 1 を送る。このとき、どの鍵管理スレーブサーバ 4 k に送るかを決める方法としては、例えば、以下の a および b に示す 2 つの方法がある。

【0073】

a. 各クライアント 2 j 毎に、どの鍵管理スレーブサーバ 4 k に鍵情報要求 6 1 を送るかを事前に決めておく方法

【0074】

b. クライアント 2 j が鍵情報要求 6 1 を送る 1 回毎に、送り先の鍵管理スレーブサーバ 4 k を変える方法（ラウンドロビン法）

【0075】

その鍵情報要求 6 1 を受け取った鍵管理スレーブサーバ 4 k 内の復号鍵送付手段 4 k 2 は、鍵情報要求 6 1 中の鍵 ID を用いて自己の鍵管理テーブル 4 k 0 の検索を行い、当該鍵 ID に対応する鍵を取得し、取得した鍵（復号鍵）とその鍵 ID との組を有する鍵情報メッセージ 6 2（図 6 参照）を、鍵情報要求 6 1 に対する返信として、鍵情報要求 6 1 を発行したクライアント 2 j に送信する。

【0076】

なお、上記以外の動作に関しては、本実施の形態に係るマルチキャスト配信のための鍵管理方式は、第 1 の実施の形態と同様の動作（処理）を行う（図 3 および図 4 参照）。

【0077】

このように、本実施の形態では、クライアント 2 j からの鍵情報要求 6 1 を受ける鍵管理スレーブサーバ 4 k が複数用意されているため、前述の第 1 の実施の形態と比べて、鍵管理サーバの負荷を分散することができる。

【0078】

（3） 第 3 の実施の形態

【0079】

図 7 は、本発明の第 3 の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【0080】

図 7 を参照すると、本実施の形態に係るマルチキャスト配信のための鍵管理方式

は、図 1 に示す第 1 の実施の形態と同様に、マルチキャストパケットを送信するコンテンツサーバ 1 1, 1 2, ..., 1 n (n は正整数) と、マルチキャストパケットを受信するクライアント 2 1, 2 2, ..., 2 m (m は正整数) と、鍵 (暗号鍵・復号鍵) の管理を行う鍵管理サーバ 3 1 と、コンテンツサーバ 1 i (i は 1 ~ n の正整数); クライアント 2 j (j は 1 ~ m の正整数), および鍵管理サーバ 3 1 を接続するネットワーク 1 0 0 とを含んで構成されている。ただし、本実施の形態におけるコンテンツサーバ 1 i は、本実施の形態に特有の構成要素として、鍵変更予告手段 1 i 3 を有している。

#### 【0081】

本実施の形態 (第 3 の実施の形態) と第 1 の実施の形態とを比較すると、本実施の形態の基本的な構成は第 1 の実施の形態 (図 1 参照) と同じであるが、コンテンツサーバ 1 i が暗号化に用いる鍵を変更する前に、事前にクライアント 2 j に対して鍵変更予告として、新たに用いる予定の鍵の鍵 ID を通知し、クライアント 2 j 側で新たな鍵情報 (復号鍵と鍵 ID との組) を事前に鍵管理サーバ 3 1 から取得しておく点が異なっている。

#### 【0082】

このような特有の構成・動作によって、コンテンツサーバ 1 i 側で暗号鍵が変わった時に、クライアント 2 j 側で遅延なく変更後の鍵による暗号化データの復号化が可能になるという特有の効果が生じる。

#### 【0083】

図 8 は、本実施の形態に係るマルチキャスト配信のための鍵管理方式の具体的な動作を説明するためのシーケンス図である。

#### 【0084】

図 9 は、本実施の形態に係るマルチキャスト配信のための鍵管理方式における鍵変更予告関連処理を示す流れ図である。この処理は、鍵変更準備時点到達認識ステップ C 1 と、鍵作成要求発行ステップ C 2 と、鍵生成ステップ C 3 と、鍵 ID 割り当てステップ C 4 と、鍵情報鍵管理テーブル保存ステップ C 5 と、鍵情報応答メッセージ送信ステップ C 6 と、鍵情報暗号鍵テーブル保存ステップ C 7 と、鍵変更予告メッセージマルチキャスト配信ステップ C 8 と、復号鍵有無判定ステ

ップC 9 と、鍵情報要求発行ステップC 1 0 と、鍵管理テーブル検索ステップC 1 1 と、鍵情報メッセージ送信ステップC 1 2 と、鍵情報復号鍵テーブル保存ステップC 1 3 とからなる。

#### 【0 0 8 5】

次に、図7～図9を参照して（図1～図4も適宜参照する）、上記のように構成された本実施の形態に係るマルチキャスト配信のための鍵管理方式の動作について、第1の実施の形態とは異なる点を中心にして説明する。

#### 【0 0 8 6】

図8に示すように、クライアント2 j（図8では、代表としてクライアント2 1を示している）は、コンテンツサーバ1 i（図8では、代表としてコンテンツサーバ1 1を示している）から、鍵IDと暗号化データとを有するマルチキャストパケットを受信し、その鍵IDに対応する鍵（復号鍵）で当該暗号化データの復号化を行っている。このような動作は、前述の第1の実施の形態における動作と同様である。

#### 【0 0 8 7】

ここで、図8に示す動作シーケンスでは、期間Aにおいては、鍵ID 1を有するマルチキャストパケット9 1（鍵ID 1で識別される暗号鍵で暗号化されたデータを有するマルチキャストパケット）が送受信されており、期間Bにおいては、鍵ID 2を有するマルチキャストパケット9 2（鍵ID 2で識別される暗号鍵で暗号化されたデータを有するマルチキャストパケット）が送受信されているものとする。

#### 【0 0 8 8】

上記のようなマルチキャストパケットの配信が行われていることを前提として、本実施の形態では、以下のような鍵変更予告関連処理が行われる（図9参照）。

#### 【0 0 8 9】

コンテンツサーバ1 i内の暗号鍵取得手段1 i 1は、ある時点（実際に新たな鍵を使用する時点よりも前の時点の任意的な時点。「鍵変更準備時点」と呼ぶ）に達したことを認識すると（ステップC 1）、新たな鍵を得るために、鍵作成要求5 1を鍵管理サーバ3 1に送る（ステップC 2）。

**【0090】**

図8の例では、コンテンツサーバ11は、鍵変更準備時点aにおいて、鍵管理サーバ31に鍵作成要求51を送信する。

**【0091】**

鍵管理サーバ31内の鍵生成手段311は、鍵作成要求51で要求された鍵（暗号鍵および復号鍵）を生成し（ステップC3）、その鍵に鍵IDを割り当て（ステップC4）、その鍵IDとその鍵との組を鍵管理テーブル310に保存し（ステップC5）、その鍵IDとその鍵（暗号鍵）との組を有する鍵情報応答メッセージ52を鍵作成要求51の発行元のコンテンツサーバ1iに送信する（ステップC6）。

**【0092】**

図8の例では、鍵管理サーバ31は、鍵2を生成し、その鍵2に鍵ID2を割り当て、鍵ID2と鍵2との組を有する鍵情報応答メッセージ52をコンテンツサーバ11に送信する。

**【0093】**

鍵情報応答メッセージ52を受信したコンテンツサーバ1i内の暗号鍵取得手段1i1は、新たな鍵の鍵情報（受け取った鍵と鍵IDとの組）を自身の暗号鍵テーブル1i0に保存する（ステップC7）。

**【0094】**

さらに、コンテンツサーバ1i内の鍵変更予告手段1i3は、新たな鍵IDと鍵との組を取得した段階で、変更後の鍵IDと鍵変更予告とを有する鍵変更予告メッセージ81のマルチキャスト配信を行う（ステップC8）。

**【0095】**

図8の例では、コンテンツサーバ11は、鍵変更予告と鍵ID2とを有する鍵変更予告メッセージ81のマルチキャスト配信を行う。

**【0096】**

鍵変更予告メッセージ81を受信した各クライアント2j内の復号鍵取得手段2j1は、当該鍵変更予告メッセージ81に含まれている鍵IDによって自身の復号鍵テーブル2j0の検索を行い、当該鍵IDに対応する鍵（復号鍵）が自身の



復号鍵テーブル 2 j 0（自テーブル）にあるか否かを判定する（ステップ C 9）。

#### 【0097】

復号鍵取得手段 2 j 1 は、ステップ C 9 の検索で「当該鍵 ID に対応する復号鍵がない」と判定した場合には、当該鍵変更予告メッセージ 8 1 に含まれる鍵 ID を使って、鍵情報要求 6 1 を鍵管理サーバ 3 1 に発行する（ステップ C 10）。すなわち、当該鍵 ID に対応する復号鍵に関する鍵情報を、鍵管理サーバ 3 1 に対して要求する。なお、ステップ C 9 の検索で「当該鍵 ID に対応する復号鍵がある」と判定した場合には、ステップ C 10 以降の処理は不要となるので、処理を終了する。

#### 【0098】

図 8 の例では、クライアント 2 1 は、鍵変更予告メッセージ 8 1 に含まれている鍵 ID 2 に対応する鍵（復号鍵）を取得するために、鍵 ID 2 を有する鍵情報要求を鍵管理サーバ 3 1 に発行する。

#### 【0099】

その鍵情報要求 6 1 を受け取った鍵管理サーバ 3 1 内の復号鍵送付手段 3 1 2 は、鍵情報要求 6 1 中の鍵 ID を用いて鍵管理テーブル 3 1 0 の検索を行い、当該鍵 ID に対応する鍵を取得する（ステップ C 11）。

#### 【0100】

その上で、復号鍵送付手段 3 1 2 は、鍵管理テーブル 3 1 0 から取得した鍵（復号鍵）とその鍵 ID との組を有する鍵情報メッセージ 6 2 を、鍵情報要求 6 1 に対する返信として、鍵情報要求 6 1 を発行したクライアント 2 j に送信する（ステップ C 12）。

#### 【0101】

当該クライアント 2 j 内の復号鍵取得手段 2 j 1 は、当該鍵情報メッセージ 6 2 を鍵管理サーバ 3 1 から受け取ると、次の期間（例えば、図 8 中の期間 A に対する期間 B）におけるマルチキャストパケット受信時の復号化処理の際に用いるために、当該鍵情報メッセージ 6 2 中の復号鍵と鍵 ID との組を自身の復号鍵テーブル 2 j 0 に保存しておく（ステップ C 13）。

**【0102】**

図8の例では、鍵管理サーバ31は、鍵ID2と鍵2との組を有する鍵情報メッセージ62をクライアント21に返信し、クライアント21は、その鍵（復号鍵）2と鍵ID2との組を自身の復号鍵テーブル210に保存する。

**【0103】**

その後（期間Bにおいて）、コンテンツサーバ11は、配信対象のデータの暗号化に鍵（暗号鍵）2を用い、鍵2で暗号化したデータと鍵ID2とを有するマルチキャストパケット92を送信する。

**【0104】**

このマルチキャストパケット92を受信したクライアント21は、鍵管理テーブル210内に保持している鍵ID2に対応する鍵（復号鍵）2を用いて、即座に暗号化データの復号化を行うことが可能になる。

**【0105】**

なお、上記以外の動作に関しては、本実施の形態においても、第1の実施の形態と同様の動作（処理）が行われる。ただし、図3および図4に示す一連の処理において、あらかじめ暗号鍵および復号鍵の取得が行われているので、上記の変更予告関連処理が正常に行われている限り、図3中のステップA2～A7の処理および図4中のステップB3～B6の処理が行われることはない。

**【0106】**

前述の第1の実施の形態では、クライアント2jは、鍵が変わった時に受信したマルチキャストパケットに含まれる鍵IDを見てはじめて鍵が変わったことを知ることになる。このため、クライアント2jは、多くの場合に、その時点で鍵管理サーバ31に新たな鍵の送付を要求し、その応答によって新たな鍵を取得することになる。このような場合に、クライアント2jは、その応答を受け取るまで、新たな鍵IDを有するマルチキャストパケット中の暗号化データの復号化ができない。

**【0107】**

これに対して、本実施の形態（第3の実施の形態）では、実際に鍵を変更する前に、コンテンツサーバ1iがクライアント2jに鍵変更予告を出しておき、あら

はじめクライアント 2 j に新たに用いる鍵を取得させておくことによって、鍵変更時に遅延なく新たな鍵による暗号化データの復号化を行うことが可能となっている。

#### 【0108】

#### (4) 第4の実施の形態

#### 【0109】

図10は、本発明の第4の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

#### 【0110】

図10を参照すると、本発明の第4の実施の形態に係るマルチキャスト配信のための鍵管理方式は、図1に示した第1の実施の形態に係るマルチキャスト配信のための鍵管理方式に対して、コンテンツサーバ用鍵管理プログラム1001、クライアント用鍵管理プログラム1002、および鍵管理サーバ用鍵管理プログラム1003を備える点が異なっている。

#### 【0111】

コンテンツサーバ用鍵管理プログラム1001は、コンテンツサーバ1iに読み込まれ、当該コンテンツサーバ1iの動作を暗号鍵テーブル1i0、暗号鍵取得手段1i1、および暗号化・送信手段1i2として制御する。コンテンツサーバ用鍵管理プログラム1001の制御によるコンテンツサーバ1iの動作（暗号鍵テーブル1i0、暗号鍵取得手段1i1、および暗号化・送信手段1i2に関する動作）は、第1の実施の形態におけるコンテンツサーバ1iの動作と全く同様になるので、その詳しい説明を割愛する。

#### 【0112】

また、クライアント用鍵管理プログラム1002は、クライアント2jに読み込まれ、当該クライアント2jの動作を復号鍵テーブル2j0、復号鍵取得手段2j1、および受信・復号化手段2j2として制御する。クライアント用鍵管理プログラム1002の制御によるクライアント2jの動作（復号鍵テーブル2j0、復号鍵取得手段2j1、および受信・復号化手段2j2に関する動作）は、第1の実施の形態におけるクライアント2jの動作と全く同様になるので、その詳

しい説明を割愛する。

#### 【0 1 1 3】

さらに、鍵管理サーバ用鍵管理プログラム 1 0 0 3 は、鍵管理サーバ 3 1 に読み込まれ、当該鍵管理サーバ 3 1 の動作を鍵管理テーブル 3 1 0，鍵生成手段 3 1 1，および復号鍵送付手段 3 1 2 として制御する。鍵管理サーバ用鍵管理プログラム 1 0 0 3 の制御による鍵管理サーバ 3 1 の動作（鍵管理テーブル 3 1 0，鍵生成手段 3 1 1，および復号鍵送付手段 3 1 2 に関する動作）は、第 1 の実施の形態における鍵管理サーバ 3 1 の動作と全く同様になるので、その詳しい説明を割愛する。

#### 【0 1 1 4】

(5) 第 5 の実施の形態

#### 【0 1 1 5】

図 1 1 は、本発明の第 5 の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

#### 【0 1 1 6】

図 1 1 を参照すると、本発明の第 5 の実施の形態に係るマルチキャスト配信のための鍵管理方式は、図 5 に示した第 2 の実施の形態に係るマルチキャスト配信のための鍵管理方式に対して、コンテンツサーバ用鍵管理プログラム 1 1 0 1，クライアント用鍵管理プログラム 1 1 0 2，鍵管理マスタサーバ用鍵管理プログラム 1 1 0 3，および鍵管理スレーブサーバ用鍵管理プログラム 1 1 0 4 を備える点が異なっている。

#### 【0 1 1 7】

コンテンツサーバ用鍵管理プログラム 1 1 0 1 は、コンテンツサーバ 1 i に読み込まれ、当該コンテンツサーバ 1 i の動作を暗号鍵テーブル 1 i 0，暗号鍵取得手段 1 i 1，および暗号化・送信手段 1 i 2 として制御する。コンテンツサーバ用鍵管理プログラム 1 1 0 1 の制御によるコンテンツサーバ 1 i の動作（暗号鍵テーブル 1 i 0，暗号鍵取得手段 1 i 1，および暗号化・送信手段 1 i 2 に関する動作）は、第 2 の実施の形態におけるコンテンツサーバ 1 i の動作と全く同様になるので、その詳しい説明を割愛する。

**【0118】**

また、クライアント用鍵管理プログラム1102は、クライアント2jに読み込まれ、当該クライアント2jの動作を復号鍵テーブル2j0、復号鍵取得手段2j1、および受信・復号化手段2j2として制御する。クライアント用鍵管理プログラム1102の制御によるクライアント2jの動作（復号鍵テーブル2j0、復号鍵取得手段2j1、および受信・復号化手段2j2に関する動作）は、第2の実施の形態におけるクライアント2jの動作と全く同様になるので、その詳しい説明を割愛する。

**【0119】**

さらに、鍵管理マスタサーバ用鍵管理プログラム1103は、鍵管理マスタサーバ40に読み込まれ、当該鍵管理マスタサーバ40の動作を鍵管理テーブル400および鍵生成・配布手段401として制御する。鍵管理マスタサーバ用鍵管理プログラム1103の制御による鍵管理マスタサーバ40の動作（鍵管理テーブル400および鍵生成・配布手段401に関する動作）は、第2の実施の形態における鍵管理マスタサーバ40の動作と全く同様になるので、その詳しい説明を割愛する。

**【0120】**

加えて、鍵管理スレーブサーバ用鍵管理プログラム1104は、鍵管理スレーブサーバ4kに読み込まれ、当該鍵管理スレーブサーバ4kの動作を鍵管理テーブル4k0、鍵保存手段4k1、および復号鍵送付手段4k2として制御する。鍵管理スレーブサーバ用鍵管理プログラム1104の制御による鍵管理スレーブサーバ4kの動作（鍵管理テーブル4k0、鍵保存手段4k1、および復号鍵送付手段4k2に関する動作）は、第2の実施の形態における鍵管理スレーブサーバ4kの動作と全く同様になるので、その詳しい説明を割愛する。

**【0121】**

(6) 第6の実施の形態

**【0122】**

図12は、本発明の第6の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

**【0123】**

図12を参照すると、本発明の第6の実施の形態に係るマルチキャスト配信のための鍵管理方式は、図7に示した第3の実施の形態に係るマルチキャスト配信のための鍵管理方式に対して、コンテンツサーバ用鍵管理プログラム1201、クライアント用鍵管理プログラム1202、および鍵管理サーバ用鍵管理プログラム1203を備える点が異なっている。

**【0124】**

コンテンツサーバ用鍵管理プログラム1201は、コンテンツサーバ1iに読み込まれ、当該コンテンツサーバ1iの動作を暗号鍵テーブル1i0、暗号鍵取得手段1i1、暗号化・送信手段1i2、および鍵変更予告手段1i3として制御する。コンテンツサーバ用鍵管理プログラム1201の制御によるコンテンツサーバ1iの動作（暗号鍵テーブル1i0、暗号鍵取得手段1i1、暗号化・送信手段1i2、および鍵変更予告手段1i3に関する動作）は、第3の実施の形態におけるコンテンツサーバ1iの動作と全く同様になるので、その詳しい説明を割愛する。

**【0125】**

また、クライアント用鍵管理プログラム1202は、クライアント2jに読み込まれ、当該クライアント2jの動作を復号鍵テーブル2j0、復号鍵取得手段2j1、および受信・復号化手段2j2として制御する。クライアント用鍵管理プログラム1202の制御によるクライアント2jの動作（復号鍵テーブル2j0、復号鍵取得手段2j1、および受信・復号化手段2j2に関する動作）は、第3の実施の形態におけるクライアント2jの動作と全く同様になるので、その詳しい説明を割愛する。

**【0126】**

さらに、鍵管理サーバ用鍵管理プログラム1203は、鍵管理サーバ31に読み込まれ、当該鍵管理サーバ31の動作を鍵管理テーブル310、鍵生成手段311、および復号鍵送付手段312として制御する。鍵管理サーバ用鍵管理プログラム1203の制御による鍵管理サーバ31の動作（鍵管理テーブル310、鍵生成手段311、および復号鍵送付手段312に関する動作）は、第3の実施の

形態における鍵管理サーバ31の動作と全く同様になるので、その詳しい説明を割愛する。

#### 【0127】

##### 【発明の効果】

以上説明したように、本発明によると、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、複数のマルチキャスト配信の各配信対象データが別々の鍵によって暗号化されている場合に、異なるそれぞれの鍵（暗号鍵・復号鍵）の管理を容易に実現することができるという効果が生じる。

#### 【0128】

このような効果が生じる理由は、コンテンツサーバが暗号化処理で使用する鍵を区別する鍵IDを、暗号化データを有するマルチキャストパケットに含めてクライアントに送り、クライアント側ではその鍵IDによってコンテンツサーバ側で暗号化に用いている鍵が変わったことを知ることができるため、暗号化に用いる鍵が変わった場合にも、クライアント側から鍵管理サーバ側に対して必要に応じて新たな復号鍵を要求することができるので、鍵管理サーバ側やコンテンツサーバ側でクライアントに関する情報の管理を行う必要がなくなるからである。

##### 【図面の簡単な説明】

#### 【図1】

本発明の第1の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

#### 【図2】

図1に示すマルチキャスト配信のための鍵管理方式の動作を説明するためのブロック図である。

#### 【図3】

図1に示すマルチキャスト配信のための鍵管理方式の暗号化・送信処理を示す流れ図である。

#### 【図4】

図1に示すマルチキャスト配信のための鍵管理方式の受信・復号化処理を示す流れ図である。

**【図 5】**

本発明の第 2 の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

**【図 6】**

図 5 に示すマルチキャスト配信のための鍵管理方式の動作を説明するためのブロック図である。

**【図 7】**

本発明の第 3 の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

**【図 8】**

図 7 に示すマルチキャスト配信のための鍵管理方式の鍵変更予告関連処理を示す流れ図である。

**【図 9】**

図 7 に示すマルチキャスト配信のための鍵管理方式の具体的な動作を説明するためのシーケンス図である。

**【図 1 0】**

本発明の第 4 の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

**【図 1 1】**

本発明の第 5 の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

**【図 1 2】**

本発明の第 6 の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

**【符号の説明】**

1 1, 1 2, …, 1 n コンテンツサーバ

2 1, 2 2, …, 2 m クライアント

3 1 鍵管理サーバ

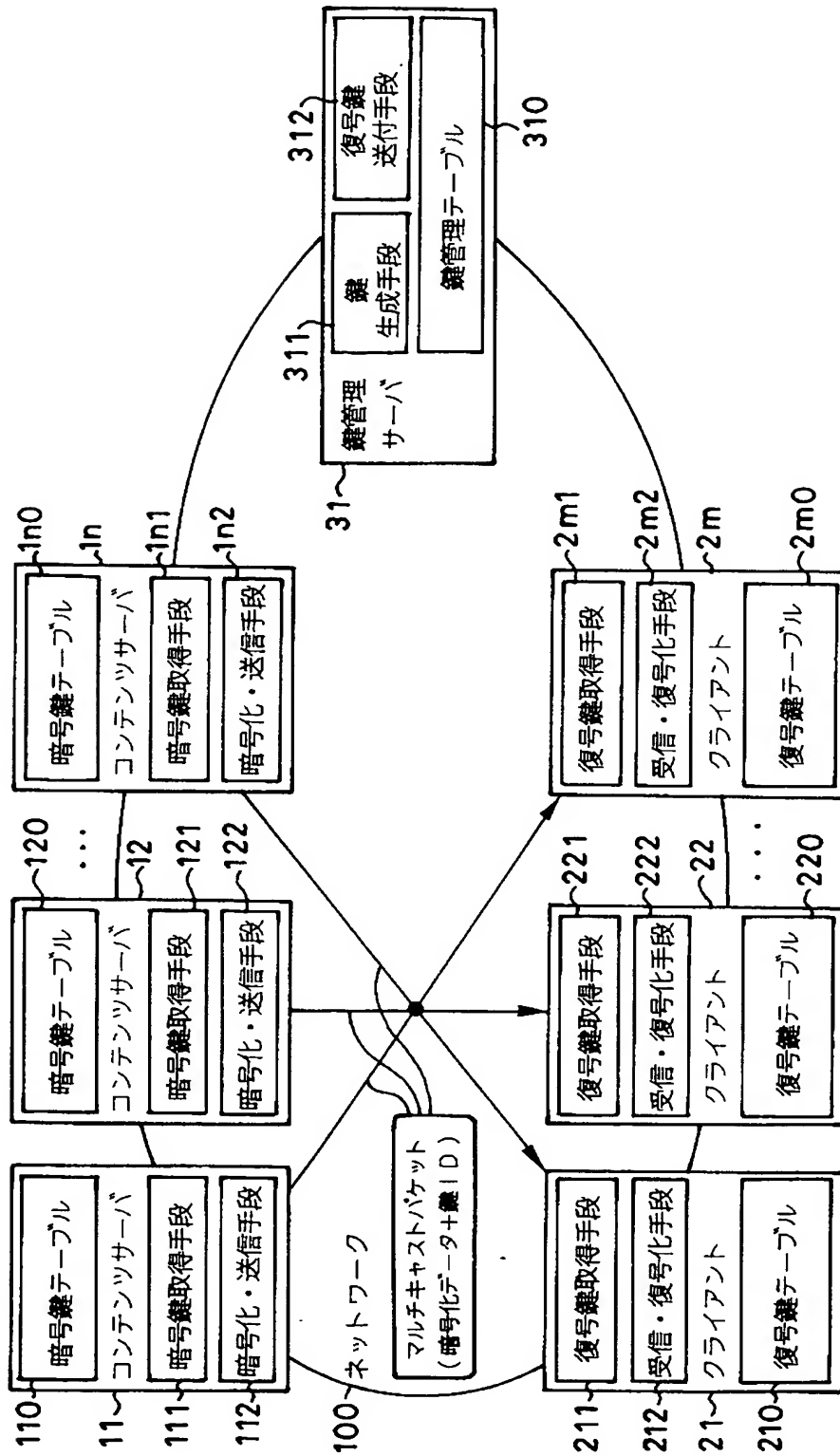
4 0 鍵管理マスタサーバ



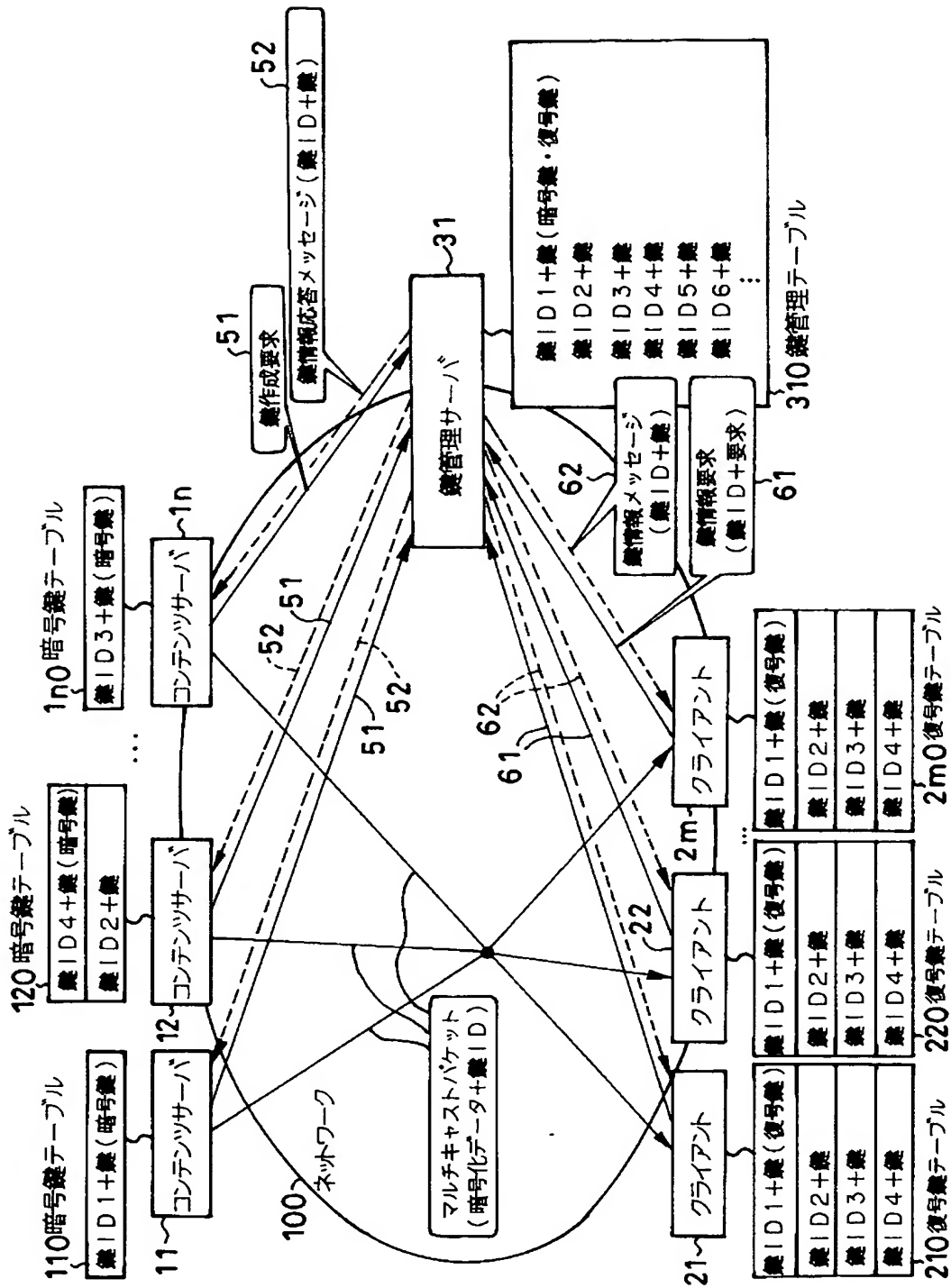
- 4 1, ..., 4 p 鍵管理スレーブサーバ
- 5 1 鍵作成要求
- 5 2 鍵情報応答メッセージ
- 6 1 鍵情報要求
- 6 2 鍵情報メッセージ
- 7 1, ..., 7 p 鍵情報配布メッセージ
- 8 1 鍵変更予告メッセージ
- 9 1, 9 2 マルチキャストパケット
- 1 0 0 ネットワーク
- 1 1 0, 1 2 0, ..., 1 n 0 暗号鍵テーブル
- 1 1 1, 1 2 1, ..., 1 n 1 暗号鍵取得手段
- 1 1 2, 1 2 2, ..., 1 n 2 暗号化・送信手段
- 1 1 3, 1 2 3, ..., 1 n 3 鍵変更予告手段
- 2 1 0, 2 2 0, ..., 2 m 0 復号鍵テーブル
- 2 1 1, 2 2 1, ..., 2 m 1 復号鍵取得手段
- 2 1 2, 2 2 2, ..., 2 m 2 受信・復号化手段
- 3 1 0, 4 0 0, 4 1 0, ..., 4 p 0 鍵管理テーブル
- 3 1 1 鍵生成手段
- 3 1 2, 4 1 2, ..., 4 p 2 復号鍵送付手段
- 4 0 1 鍵生成・配布手段
- 4 1 1, ..., 4 p 1 鍵保存手段
- 1 0 0 1, 1 1 0 1, 1 2 0 1 コンテンツサーバ用鍵管理プログラム
- 1 0 0 2, 1 1 0 2, 1 2 0 2 クライアント用鍵管理プログラム
- 1 0 0 3, 1 2 0 3 鍵管理サーバ用鍵管理プログラム
- 1 1 0 3 鍵管理マスタサーバ用鍵管理プログラム
- 1 1 0 4 鍵管理スレーブサーバ用鍵管理プログラム

【書類名】 図面

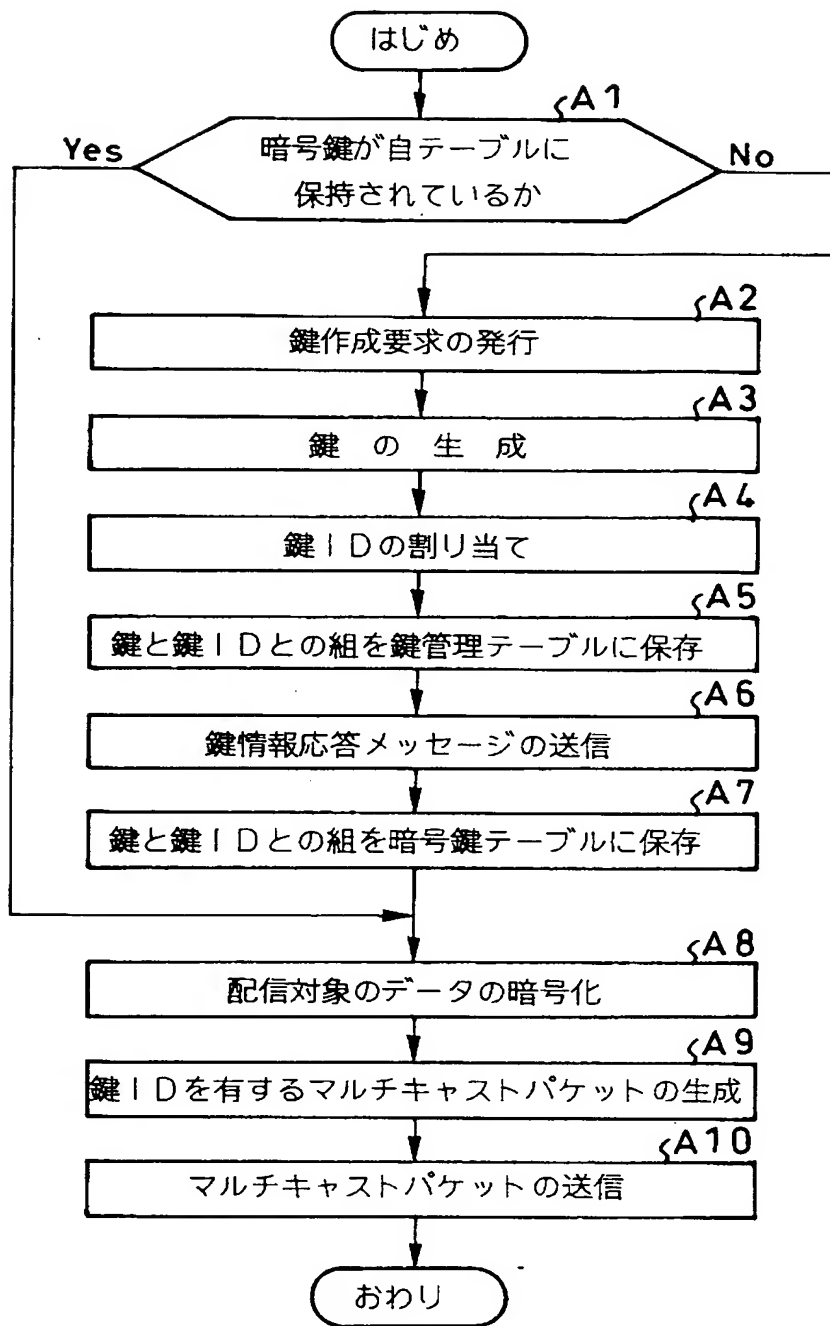
【図 1】



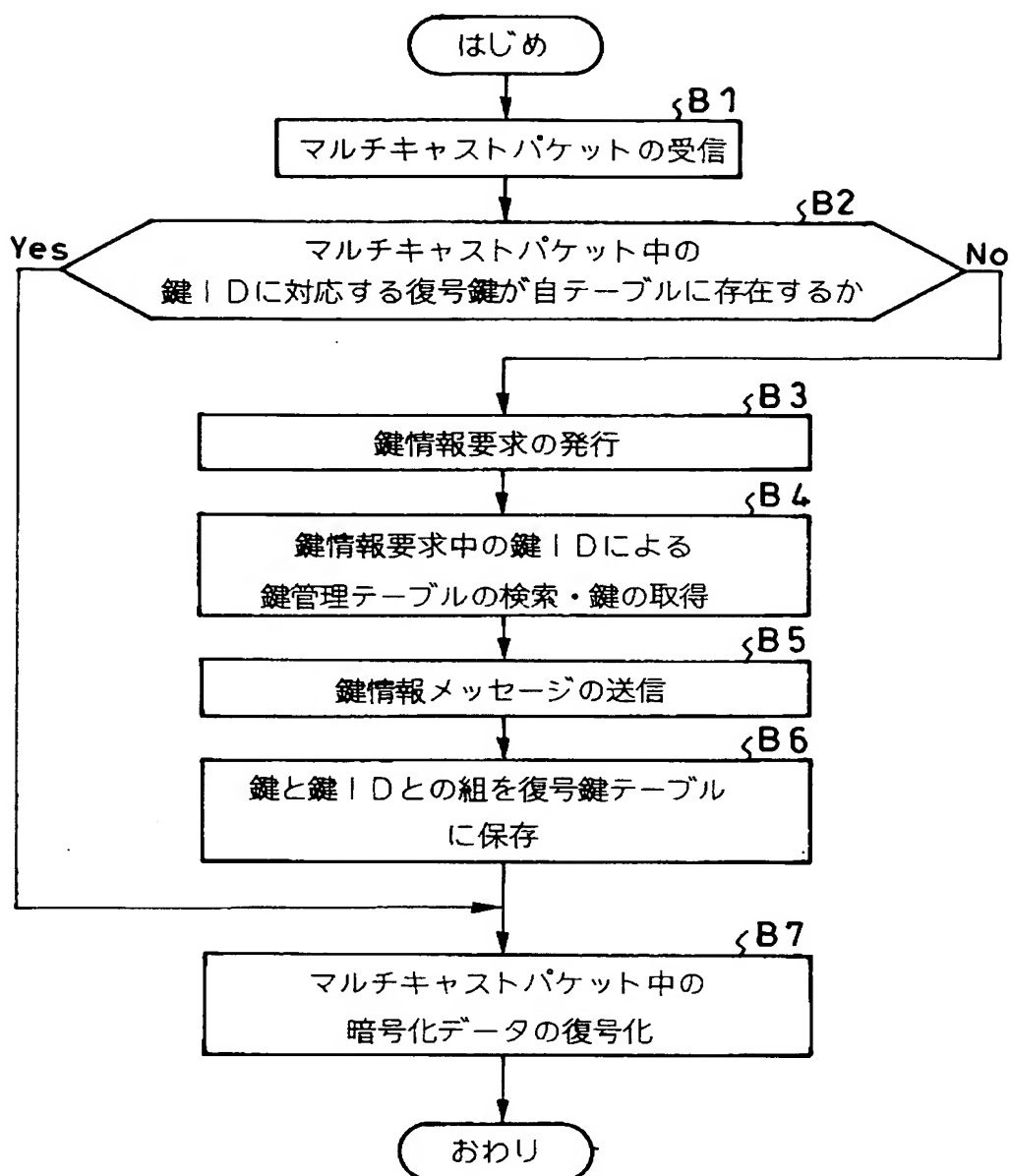
【図 2】



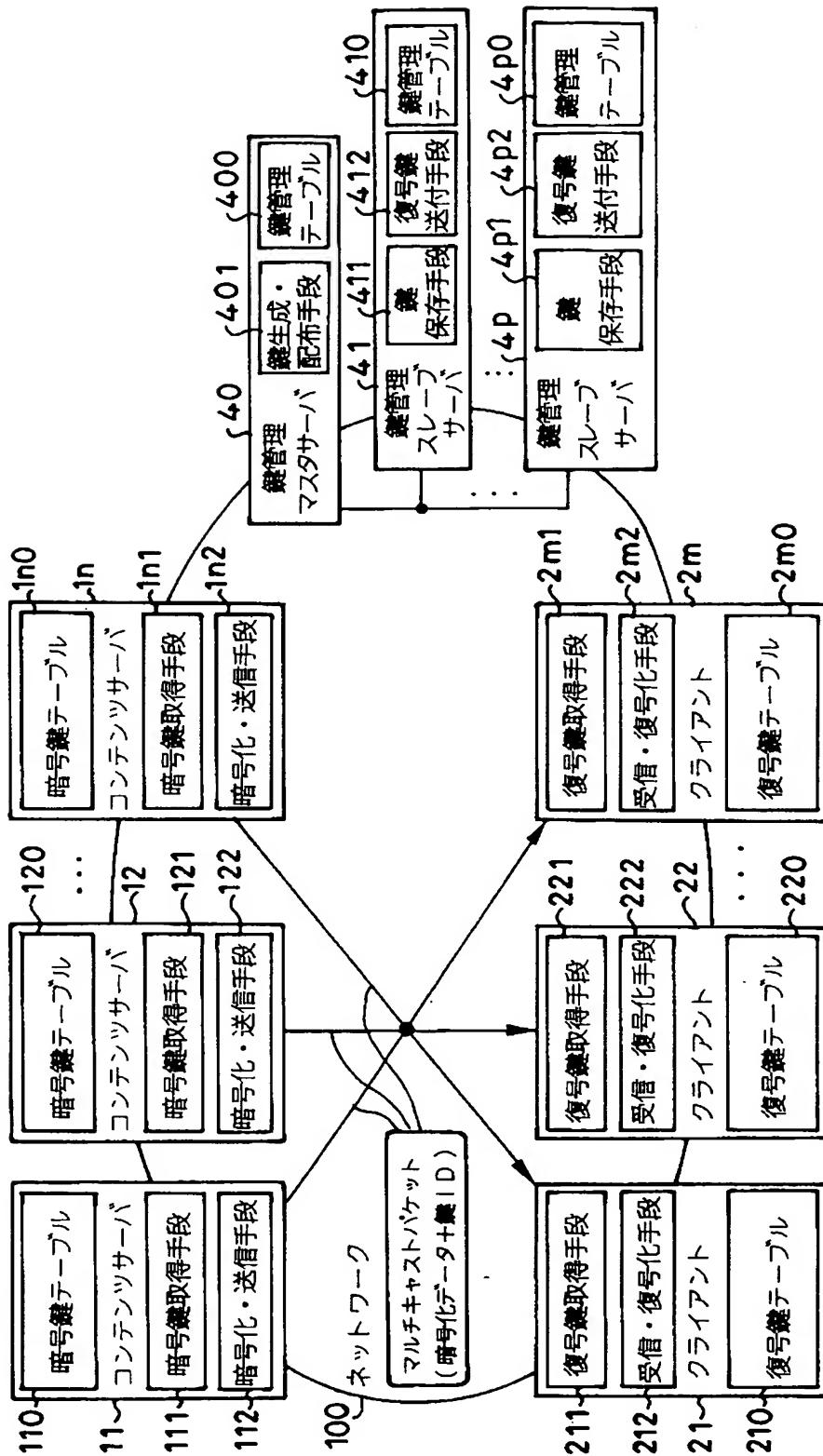
【図 3】



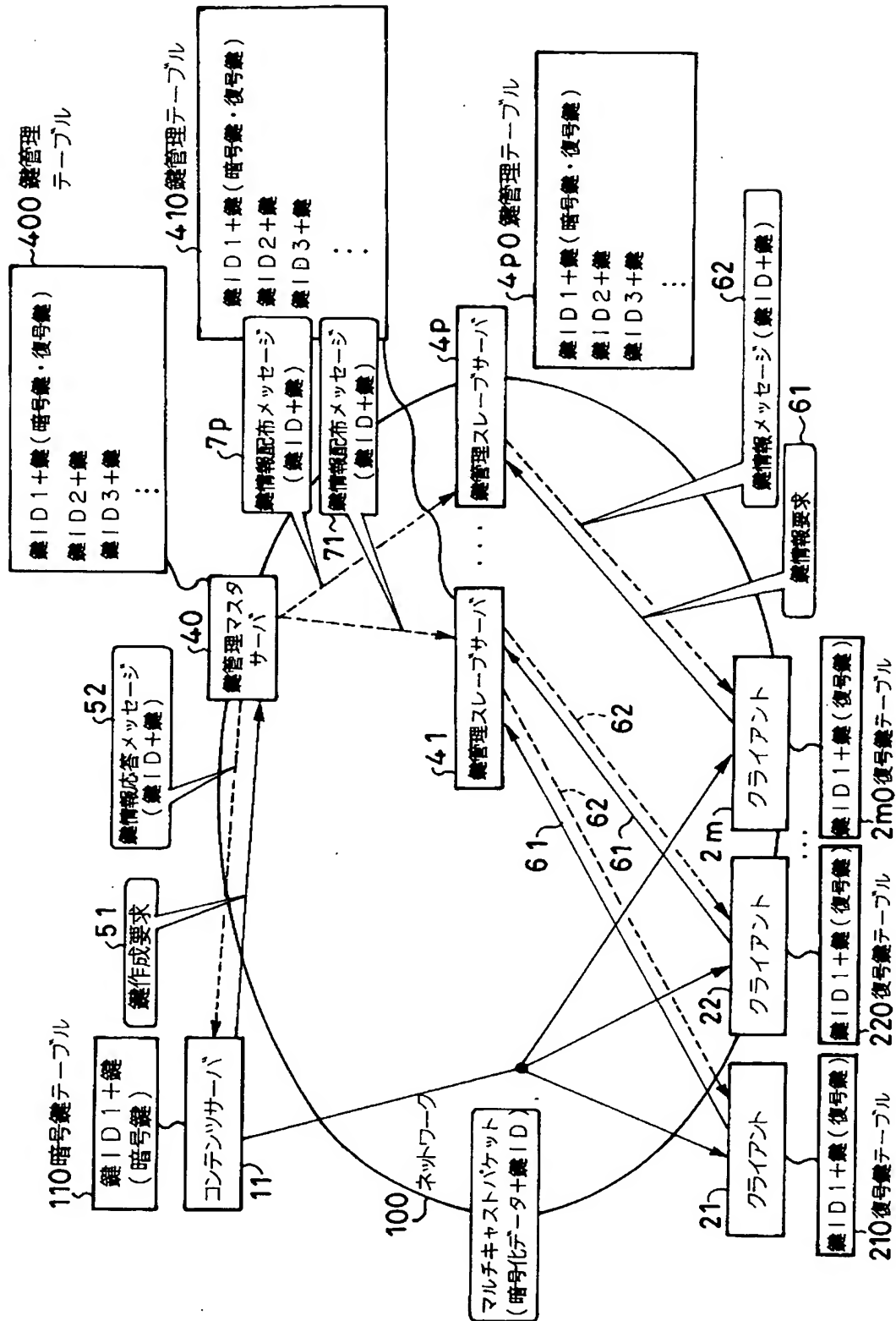
【図 4】



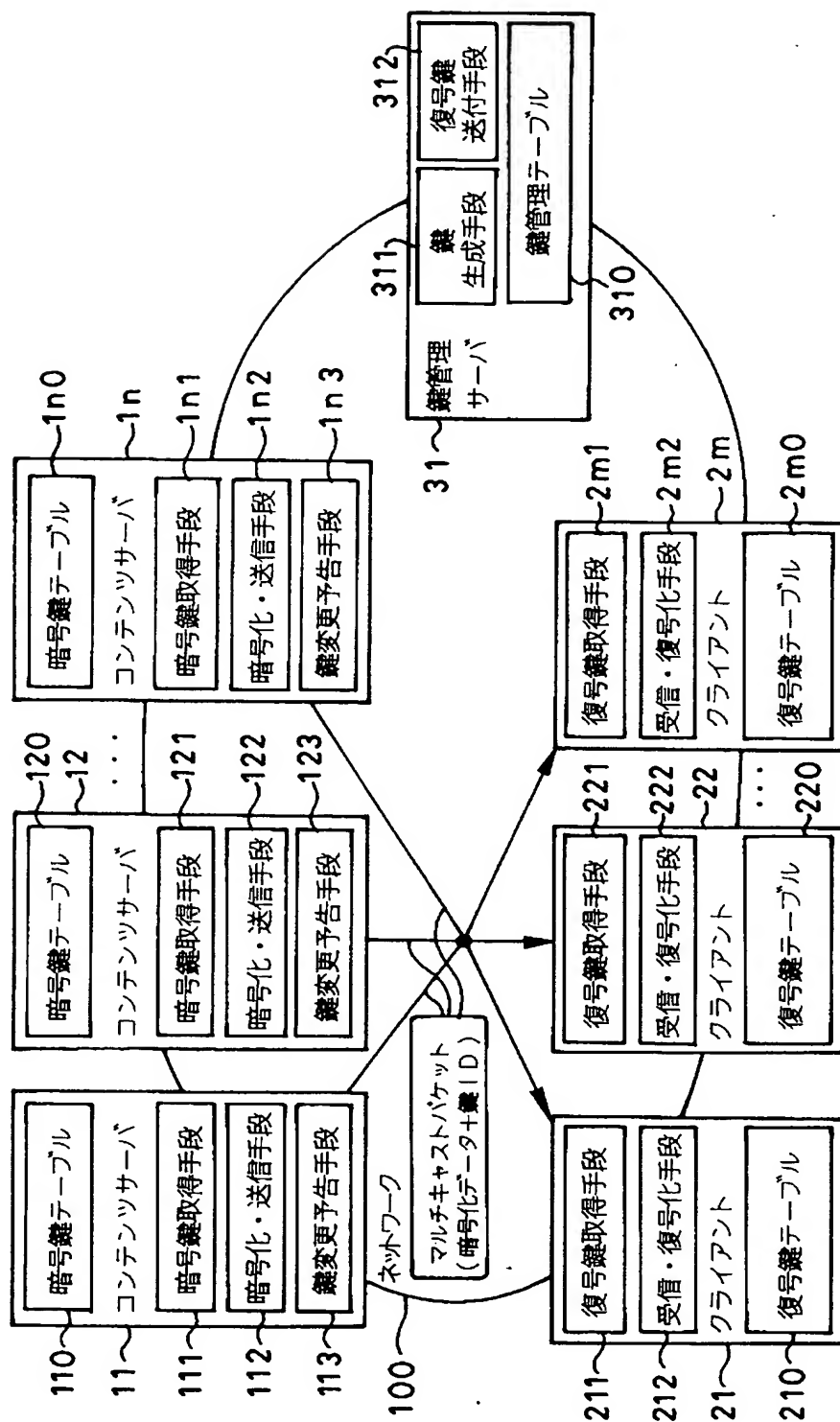
【図 5】



【図6】

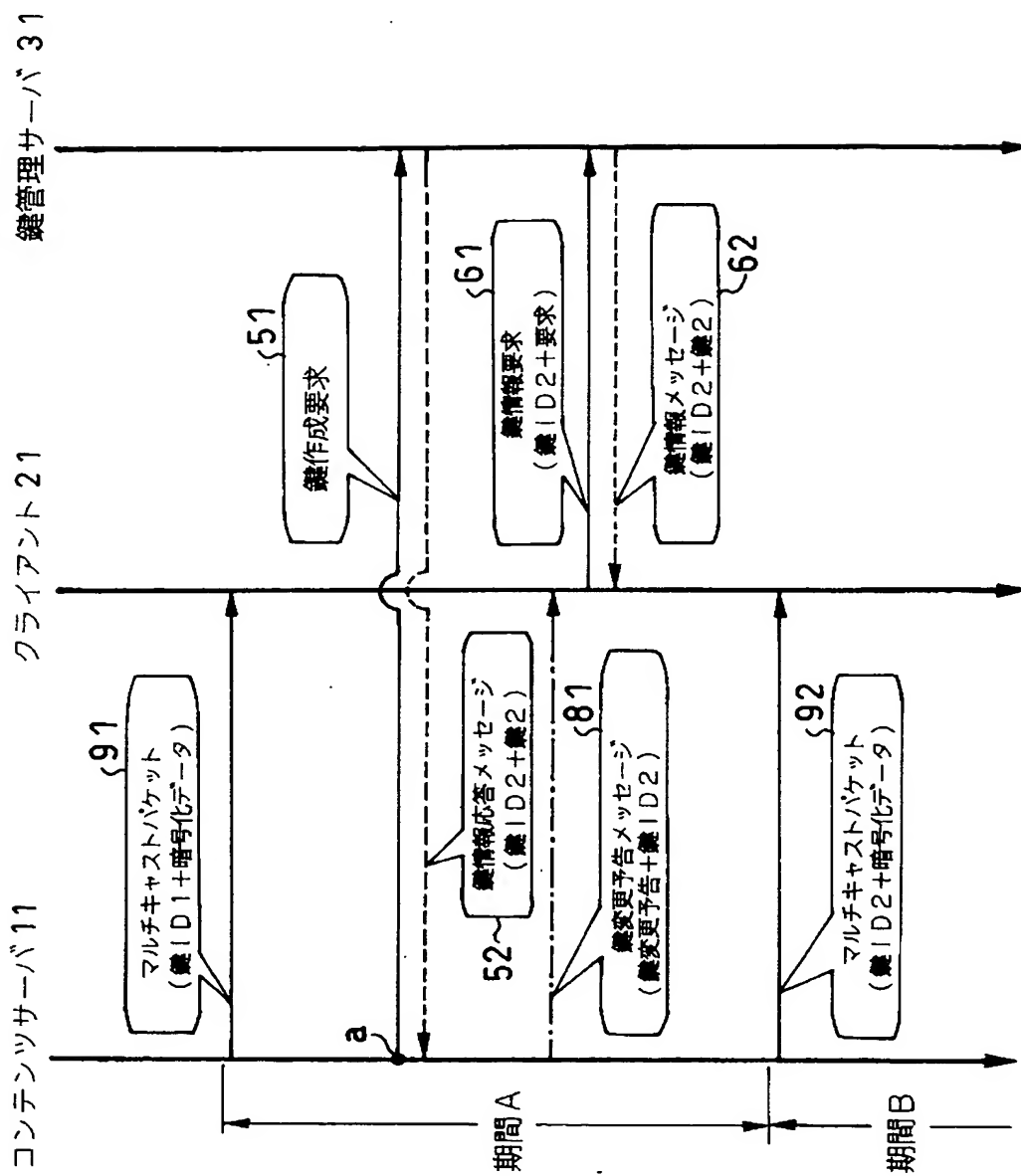


【図 7】

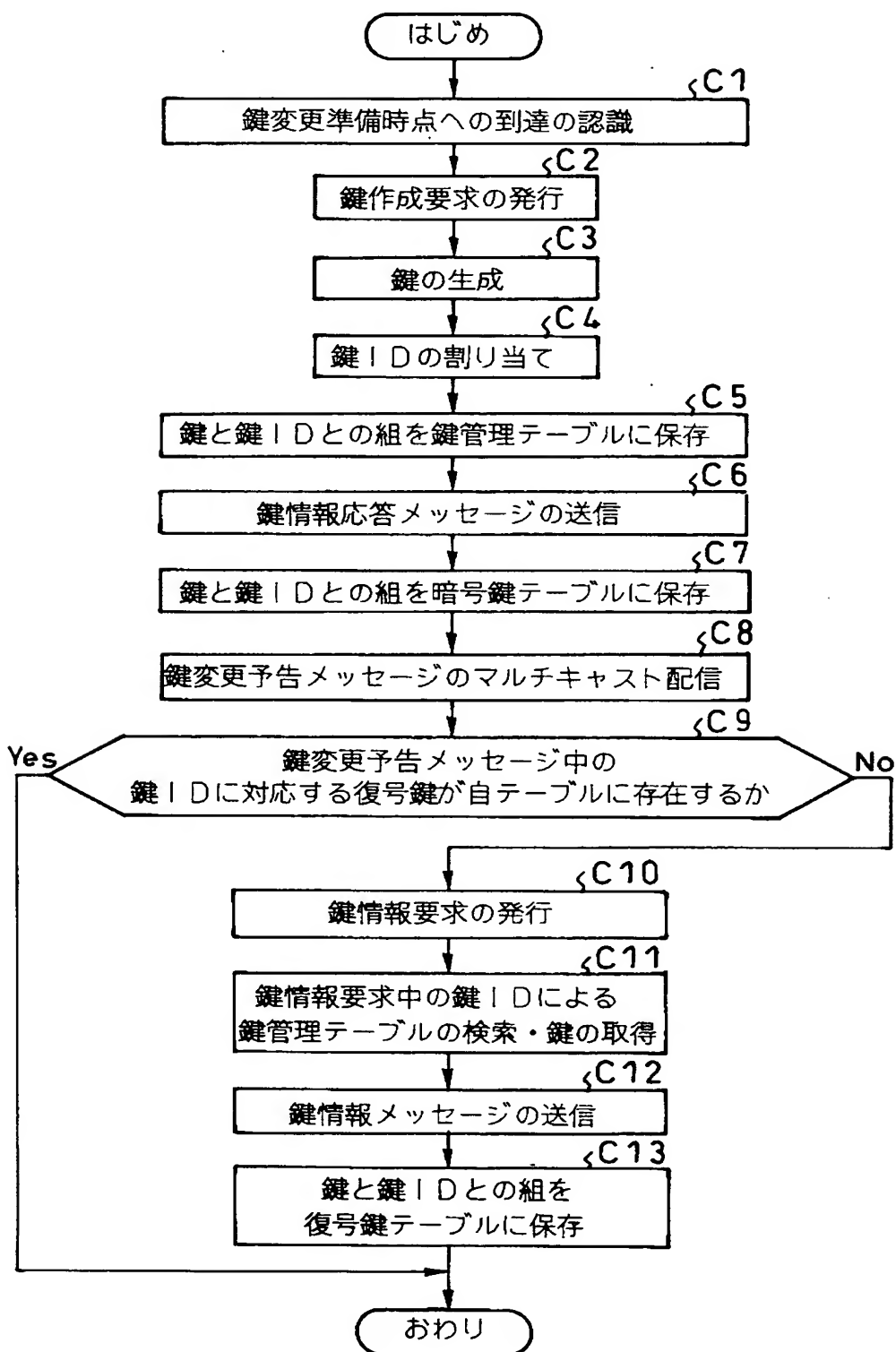




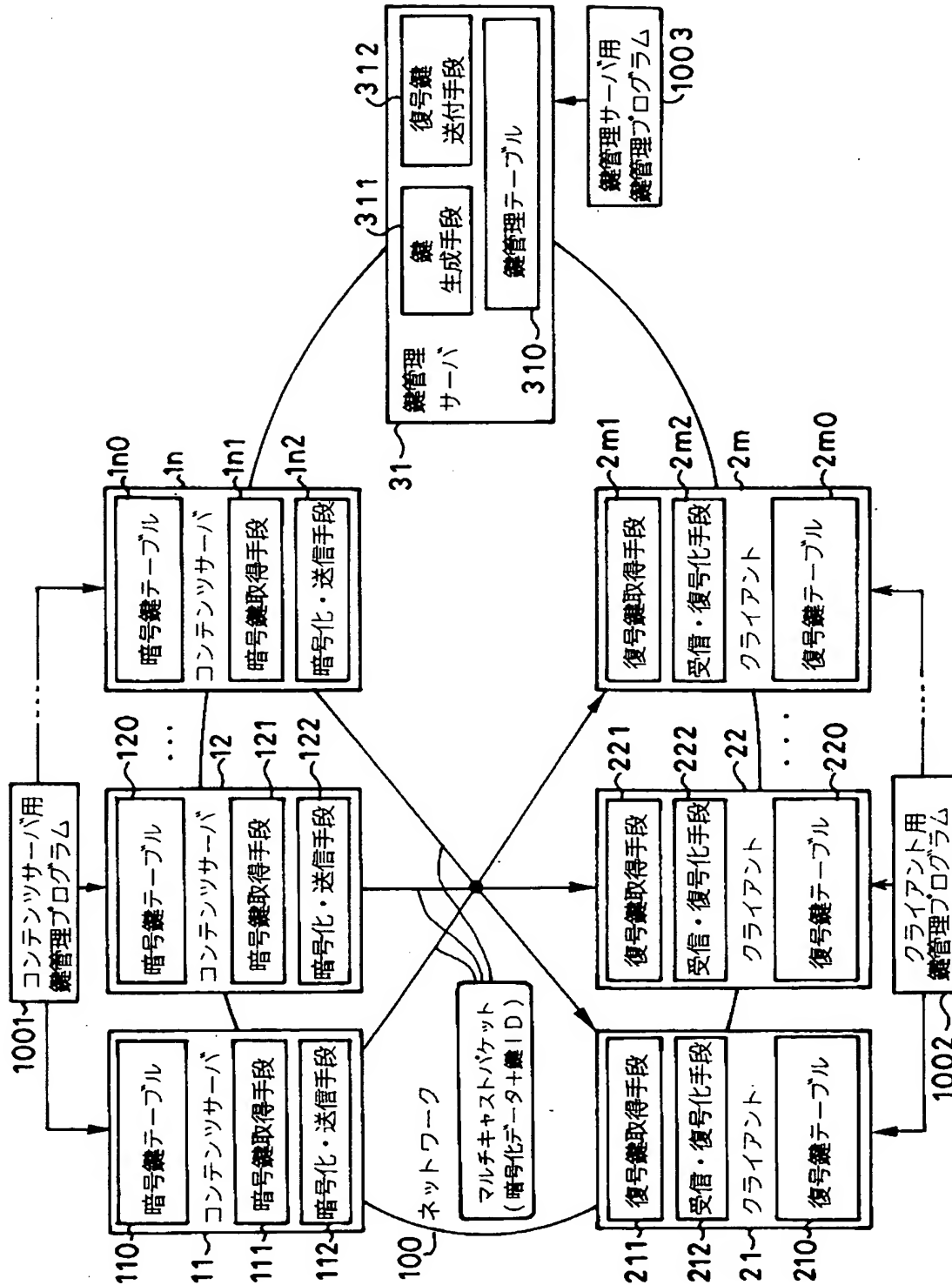
【図8】



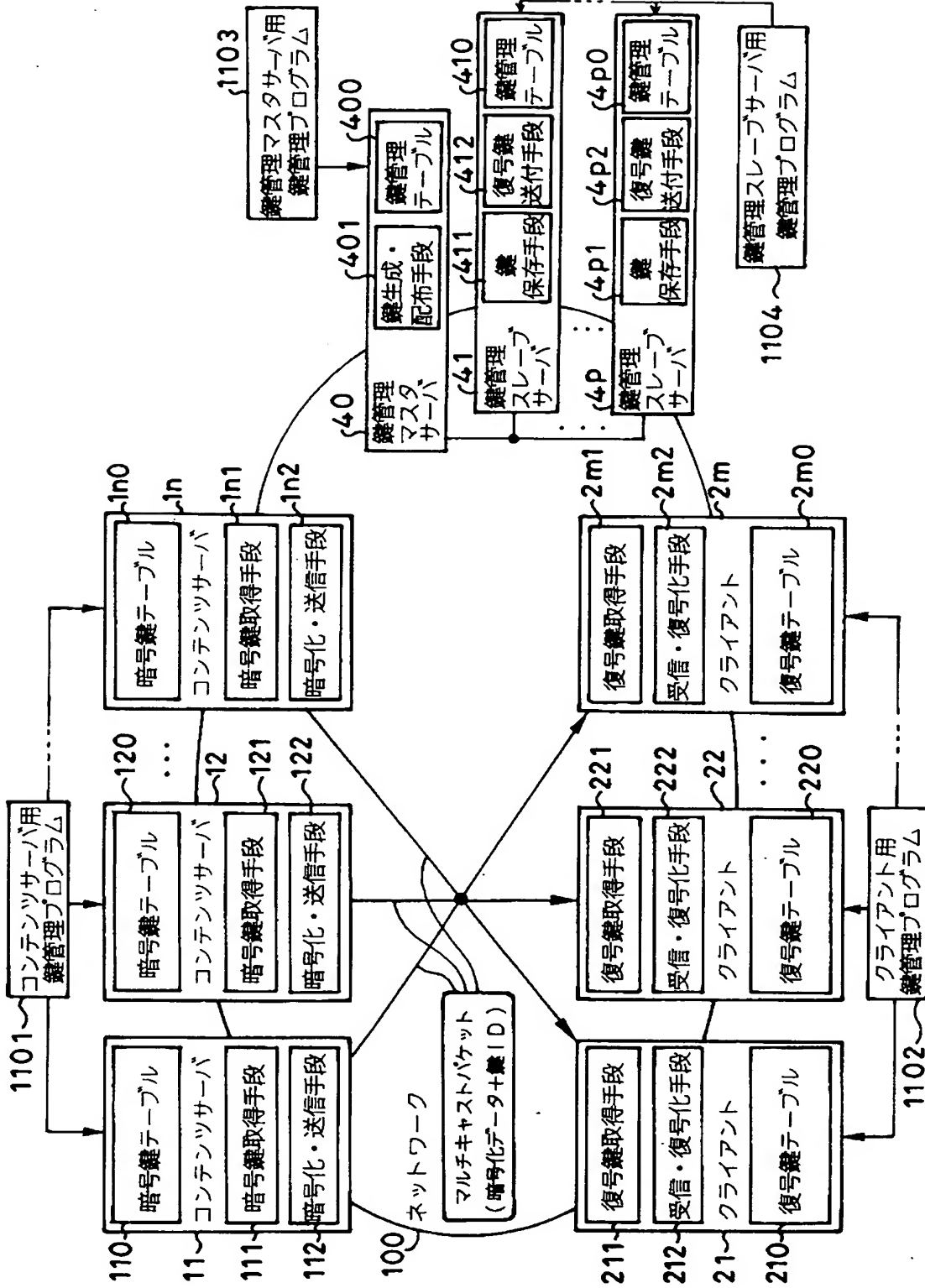
【図 9】



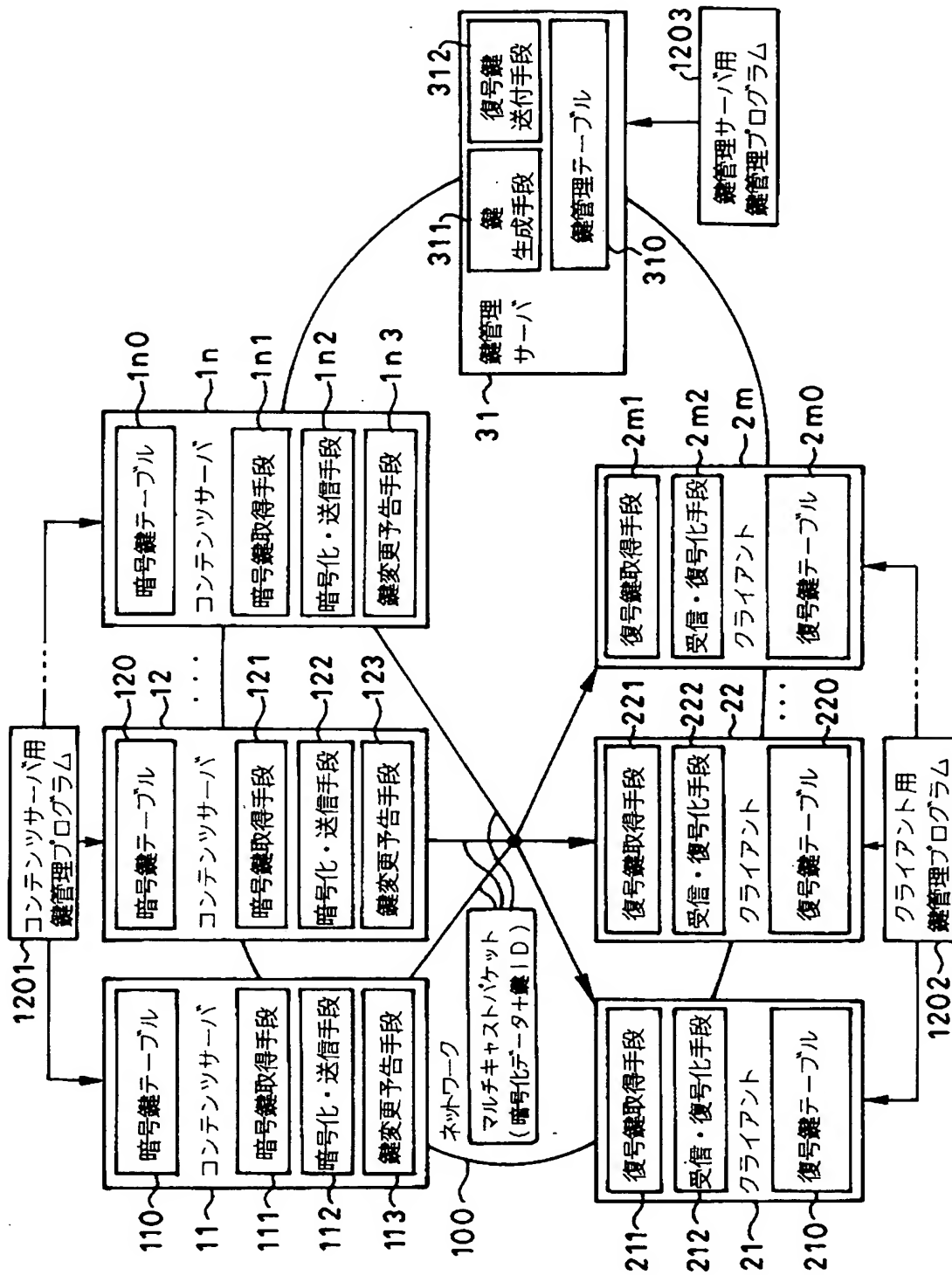
【図10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおける鍵（暗号鍵／復号鍵）の管理を容易に実現できるようにする。

【解決手段】 鍵管理サーバ 3 1 は、暗号鍵・復号鍵と当該鍵を一意に識別するための鍵 I D との組を保持することによって鍵を管理する。コンテンツサーバ 1 1 ～ 1 n の各々は、鍵管理サーバ 3 1 から暗号鍵とその鍵 I D との組を受け取り、当該暗号鍵で暗号化されたデータと当該鍵 I D とを有するマルチキャストパケットをクライアント 2 1 ～ 2 m に送信する。クライアント 2 1 ～ 2 m の各々は、コンテンツサーバ 1 1 ～ 1 n からマルチキャストパケットを受信し、当該マルチキャストパケットに含まれる鍵 I D に対応する復号鍵を鍵管理サーバ 3 1 から取得し、当該復号鍵によって当該マルチキャストパケットに含まれる暗号化データの復号化を行う。

【選択図】 図 1

## 認定・付加情報

|         |                |
|---------|----------------|
| 特許出願の番号 | 特願 2002-332405 |
| 受付番号    | 50201731559    |
| 書類名     | 特許願            |
| 担当官     | 第八担当上席 0097    |
| 作成日     | 平成14年11月18日    |

## &lt;認定情報・付加情報&gt;

|       |             |
|-------|-------------|
| 【提出日】 | 平成14年11月15日 |
|-------|-------------|

次頁無

特願 2 0 0 2 - 3 3 2 4 0 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 4 2 3 7 ]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社